THE IMPACT OF EXTENDING THE DEFENSE MESSAGE SYSTEM TO THE ARMY WARFIGHTER

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE

by

ANTHONY E. BLANDO, MAJ, USA
B.A., UNIVERSITY OF WISCONSIN, MILWAUKEE, WISCONSIN, 1984

Fort Leavenworth, Kansas
1996

THE IMPACT OF EXTENDING THE DEFENSE MESSAGE SYSTEM TO THE ARMY WARFIGHTER

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE

by

ANTHONY E. BLANDO, MAJ, USA
B.A., UNIVERSITY OF WISCONSIN, MILWAUKEE, WISCONSIN, 1984

Fort Leavenworth, Kansas
1996

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: MAJ Anthony E. Blando

Thesis Title: The Impact of Extending The Defense Message System to the Army Warfighter

Approved by:

______________________________, Thesis Committee Chairman
MAJ Howard R. Cuozzi, M.F.A.

______________________________, Member
SPC John T. Broom, Ph.D.

______________________________, Member
LTC Keith B. Harker, M.S.

Accepted this 7th day of June 1996 by:

______________________________, Director, Graduate Degree Programs
Philip J. Brookes, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other government agency. (References to this study should include the foregoing statement.)

ABSTRACT

THE IMPACT OF EXTENDING THE DEFENSE MESSAGE SYSTEM TO THE ARMY WARFIGHTER by Anthony E. Blando, USA, 100 pages.

The Department of Defense is transitioning the current Automatic Digital Network (AUTODIN) and Electronic Mail (E-mail) systems to the Defense Message System (DMS). When fully implemented, users will be able to draft, send, receive, and read messages of all classifications from a single personal computer or command and control workstation. The DMS replaces the current manpower and resource intensive messaging systems used today. The impact on the Army is, no more Telecommunications Centers, AUTODIN Switching Centers, Tactical Message Switches, Mobile Gateway Vans, or homegrown E-mail systems.

The purpose of this thesis is to describe the DMS concept, requirements, and components; describe the tactical DMS transition strategy; and assess the impact of extending DMS to the battlefield. The criteria used for assessment are: doctrine, training, leader development, organizations, material, and soldiers (DTLOMS).

The DMS will significantly enhance the tactical commanders capabilities. Conversely, there will be a number of impacts created by this system. To ensure a successful transition, DMS planners and leaders at all levels must understand and address many unique tactical concerns and requirements in each area of the DTLOMS.

TABLE OF CONTENTS

LIST OF ACRONYMS

ABCS	Army Battle Command System
ACUS	Army Common User System
ADUA	Administrative Directory User Agent
AFATDS	Advanced Field Artillery Tactical Data System
AGCCS	Army Global Command and Control System
AKMS	Army Key Management System
AIG	AUTODIN Indicator Group
ASAS	All Source Analysis System
ASB	Army Science Board
ASC	AUTODIN Switching Center
ASDC3I	Assistant Secretary of Defense for C3I
ATCCS	Army Tactical Command and Control System
ATM	Asynchronous Transfer Mode
AUTODIN	Automatic Digital Network
C2	Command and Control
C3	Command Control and Communications
C3I	C3 and Intelligence
C4	Command Control Communications and Computers
C4I	C4 and Intelligence
CA	Certification Authority
CAD	Collective Address Designators
CALL	Center For Army Lessons Learned
CAW	Certification Authority Workstation

CECOM	Communications Electronics Command
CHS2	Common Hardware Software II
COTS	Commercial Off The Shelf
CT	Communications Terminal
CSSCS	Combat Service Support Control System
DCS	Defense Communication System
DDN	Defense Data Network
DIL	Digital Integration Laboratory
DINAH	Desktop Interface to AUTODIN Host
DISC4	Director of Information Systems for C4
DISN	Defense Information Systems Network
DMS	Defense Message System
DOD	Department of Defense
DSA	Directory Service Agent
DSS	Digital Signature Standard
DSSCS	Defense Special Security Communications System
DTLOMS	Doctrine, Training, Leader development, Organizations, Material, and Soldiers
DUA	Directory User Agent
ESOP	Enhanced Switch Operations Position
FAADC3I	Forward Area Air Defense C3I System
FES	Forced Entry Switch
FRD	Functional Requirements Document
FTP	File Transfer Protocol
GCCS	Global Command and Control System
GENSER	General Service
GOSIP	Government Open Systems Interconnect Profile
IMTA	Intermediate Message Transfer Agent

INE	Inline Network Encryptor
IOT&E	Initial Operational Test & Evaluation
ISC	Information Systems Command
ISDN	Integrated Services Digital Network
ISYSCON	Integrated Systems Control
JANAP	Joint Army and Navy and Air Force Procedures
JCSE	Joint Communications Support Element
JTIC	Joint Test and Interoperability Center
JWICS	Joint Warrior Intelligence Communications System
JWID	Joint Warrior Interoperability Demonstration
LAN	Local Area Network
LEN	Large Extension Node
MACOM	Major Command
MCS	Maneuver Control System
MFI	Multifunctional Interpreter
MGV	Mobile Gateway Van
MI	Military Intelligence
MILNET	Military Network
MISSI	Multilevel Information Systems Security Initiative
MLA	Mail List Agent
MLS	Multilevel Security
MROC	Multicommand Required Operational Capabilities
MS	Message Store
MSE	Mobile Subscriber Equipment
MTA	Message Transfer Agent
MWS	Management Workstation
NCA	National Command Authority
NCS	Node Center Switch

NES	Network Encryption System
NICP	National Inventory Control Point
NIPR	Nonclassified Internet Protocol Router
NIST	National Institute for Standards and Technology
NOS	Network Operating System
NSA	National Security Agency
NTC	National Training Center
OA	Operational Architecture
OPFAC	Operational Facility
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PEO	Program Executive Office
PIN	Personal Identification Number
PM	Project Manager
PMJTACS	Program Manager for Joint Tactical Communications Systems
RARP	Reverse Address Resolution Protocol
RFC	Request For Comment
RFP	Request For Proposal
ROMC	Required Operational Messaging Characteristics
SA	Systems Architecture
SBU	Sensitive But Unclassified
SCI	Special Compartmented Information
SCIF	Special Compartmented Information Facility
SEN	Small Extension Node
SHA	Secure Hash Algorithm
SHTU	Simplified Handheld Terminal Unit
SIGCEN	Signal Center
SINCGARS	Single Channel Ground and Airborne Radio System

SIPR	Secret Internet Protocol Router
SMTP	Simple Mail Transfer Protocol
SNS	Secure Network Server
STAMIS	Standard Army Management Information System
STDN	Secure Tactical Data Network
STEP	Standardized Tactical Entry Point
TA	Technical Architecture
TACWG	Tactical Working Group
TAIS	Target Architecture and Implementation Strategy
TDMS	Tactical Defense Message System
TG	Tactical Guard
TMG	Tactical Multinet Gateway
TNS	Tactical Name Server
TPN	Tactical Packet Network
TOC	Tactical Operations Center
TRADOC	Training and Doctrine Command
TRITAC	Tri-Services Tactical Communications
TRTS	Tactical Record Traffic System
TS	Top Secret
TTA	Telephone Terminal Adaptor
TWG	Tactical Working Group
UA	User Agent
USAISC	U.S. Army Information Systems Command
USMTF	U.S. Message Text Format
WAN	Wide Area Network
WWMCCS	Worldwide Military Command and Control System
WWW	World Wide Web

LIST OF ILLUSTRATIONS

CHAPTER 1

INTRODUCTION

The United States Army's Enterprise Strategy is the single, unified vision for the Army Command Control Communications, Computers and Intelligence (C4I) community. Its purpose is to integrate current Army doctrine and modernization plans for the evolution of information systems to "Win the Battlefield Information War."[1] This strategy is based on ten principles designed to ensure the future warfighter's ability to maintain information superiority over any opponent.

Optimize the Information Technology Environment is principle six, its purpose is to provide the warfighter more efficient information support for combat and peacetime operations. Implement Multilevel Security (MLS), principle seven, is based on the Army's ability to provide the warfighter a system to access and exchange information at needed levels of classification using a single C4I platform.[2]

The Army has always used information technology. The Army cannot, however, access and exchange information at needed levels of classification using a single platform. Today the Army needs several different computers connected to several different networks to send different messages at various security classification levels. Figure 1 represents the Army's current messaging architecture. There are many initiatives underway to solve this problem. The Defense Message

System (DMS) is one and the National Security Agency's (NSA) Multilevel Information Systems Security Initiative (MISSI) program

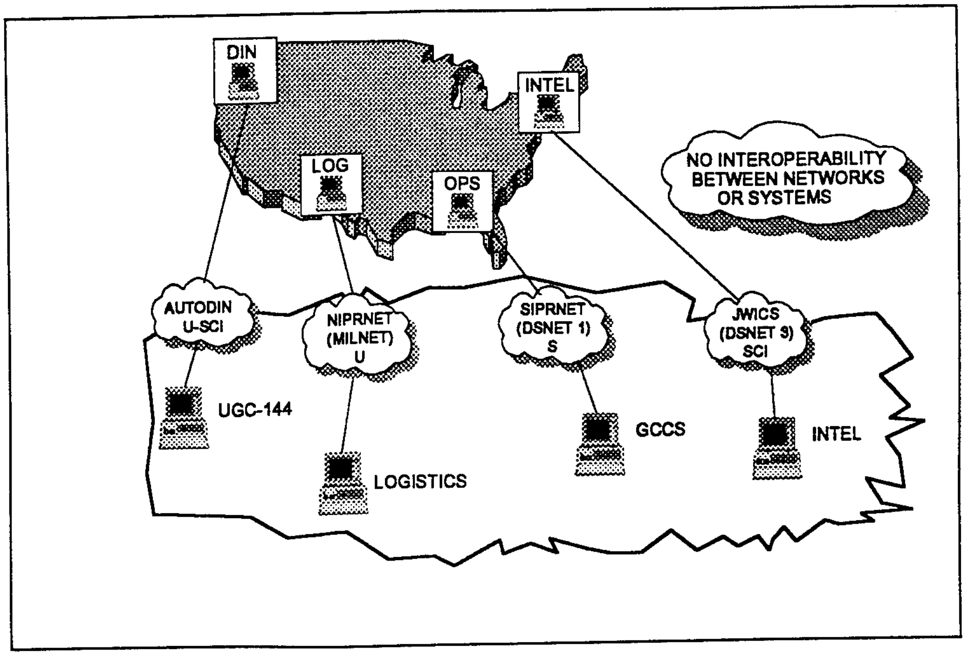

Figure 1. Current Messaging Architecture

is another. The DMS optimizes the information technology environment and MISSI will provide the tools to achieve MLS. The two combined will provide the warfighter a system to access and exchange information at needed levels of classification using a single C4I system.

The Department of Defense is transitioning the current AUTODIN and Electronic Mail (E-mail) systems to the DMS. When fully implemented, users will be able to draft, send, receive, and read messages from a single personal computer or Command and Control (C2) workstation. The DMS replaces the current manpower and resource intensive messaging systems used today. The impact on the Army is:

no more Telecommunications Centers, AUTODIN Switching Centers, Tactical Message Switches (TYC-39s), Mobile Gateway Vans, or homegrown E-mail systems. Figure 2 represents the future messaging architecture with DMS.

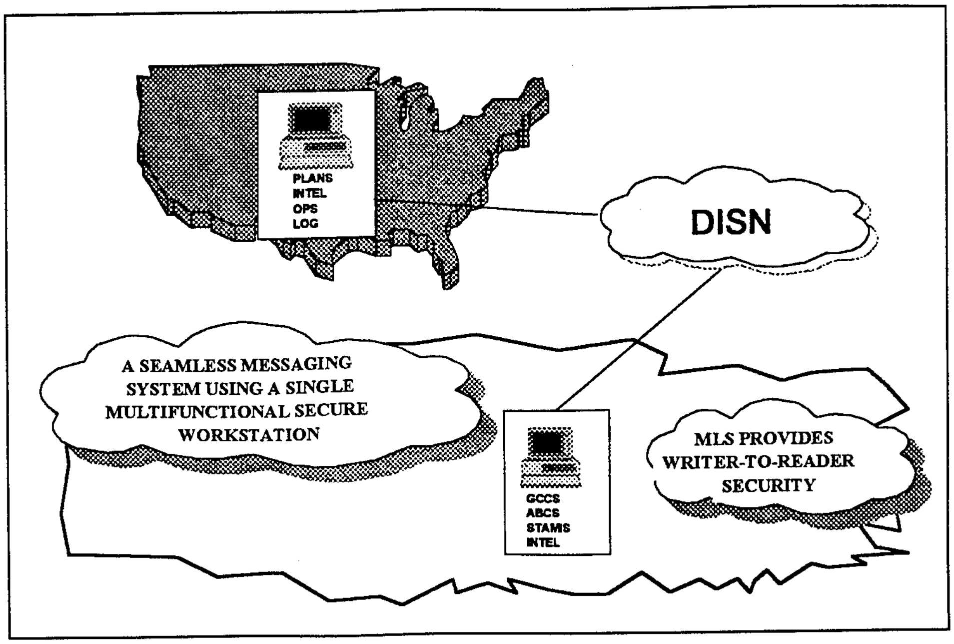

Figure 2. Messaging With DMS

The DMS program was conceived in 1988, but it was not until 1994 that tactical users were integrated into the DMS planning community.[3] Subsequently, the tactical Army lagged far behind the sustaining base in identifying requirements and developing a clear transition plan for users on the battlefield. Recently, the Signal Center at Fort Gordon, Georgia, and the United States Army Information Systems Command (USAISC) developed a strategy for transitioning the Tactical Record Traffic System (TRTS) to the Tactical DMS system.[4] They also identified unique tactical requirements the DMS must satisfy. What DMS planners have not done is assess the impact of extending DMS to the battlefield.

The purpose of this thesis is to describe the DMS concept, requirements, and components; describe the Tactical DMS transition strategy; and assess the impact of extending DMS to the battlefield. Because of the technical nature of this thesis, it will primarily target the impact on the Wide Area Network (WAN) installers, operators, maintainers, and managers. That is, the Signal Corps and other information system providers. The criteria this thesis will use for assessment are: doctrine, training, leader development, organizations, material, and soldiers (DTLOMS).

Definitions of Criteria

Doctrine

Doctrine is defined as the fundamental principles by which users send and receive messages across the battlefield and to the sustaining base. This includes management, message flow, installation, operation, and maintenance of components, and message dissemination. Doctrine also includes policy that affects messaging on the battlefield.

Training

This is the training required for installation, operation, maintenance, and management of all DMS messaging components. This includes institutional, embedded, and sustainment training required for the Signal Corps, as well as end users.

Leader Development

This criteria defines the roles and responsibilities leaders play in the installation, operation, maintenance, and management of messaging components.

Organizations

This is the organizational structure required to install, operate, maintain, and manage the DMS components. This includes the number of soldiers required today and the number required for DMS. It also includes new positions required and positions no longer required.

Material

This is all the equipment required to install, operate, maintain, and manage the DMS components. It includes all hardware, software, and security components required for DMS. It also includes the impact on bandwidth.

Soldiers

This criteria primarily focuses on the enlisted soldiers required to install, operate, maintain, and manage the DMS components. This includes the specific MOS requirements and any additional training or retraining that soldiers may have to undergo once DMS is implemented.

Why the Army is Implementing DMS

Today there are two message classes: organizational (AUTODIN) and individual (E-mail). AUTODIN is based on 30-year-old technology, is extremely expensive to run, and requires high staffing levels. E-mail is currently provided by Simple Mail Transfer

Protocol (SMTP) based systems and a multitude of other proprietary Local Area Network (LAN) based systems.[5]

The current method of moving formal messages across the battlefield and to the sustaining base is very complex. If a warfighter at a maneuver brigade wants to send a formal message to someone in the sustaining base, he either drives or walks the message to someone at the division level with a communications terminal (CT). The CT operator inputs the message and sends it to a message switch via the Mobile Subscriber Equipment (MSE) and Tri-Service Tactical (TRITAC) networks. Eventually, the message will be sent to an AUTODIN Switching Center (ASC) and then a local Communications Center (COMCEN). If the message is unclassified it will be converted to E-mail and delivered to the intended recipient. If the message is classified secret or above, the message must be picked up. If the intended recipient replies, he drafts the message and gives it to his secretary. The secretary types the message on the Desktop Interface to the AUTODIN Host (DINAH) terminal and then either walks or drives the message to the COMCEN to begin the long, slow journey back to the warfighter.

The methods currently used to send informal E-mail from the battlefield to the sustaining base are equally complex. Two of the methods used today are the Mobile Gateway Van (MGV), or the Deployable Automation System Host (DASH). Both are E-mail hosts mounted in shelters on the back of tactical vehicles. They were used extensively in Somalia and Haiti and will be used in Bosnia. They have worked well and have somewhat satiated the current appetite for E-mail on the battlefield. The problems are not so much the complexity of installing the system, rather the cost of doing so.

First, there are no designated MOSs to operate these systems so the signal brigades must operate them with soldiers who would normally be performing other duties. Second, both the MGV and DASH use the circuit switch rather than the packet switch or Tactical Packet Network (TPN). This is significant because the bandwidth allocated to the circuit switch is designed for telephone or facsimile calls. E-mail users on the circuit switch could quickly consume a large portion of the bandwidth commanders use to command and control their forces by voice.[6]

In addition to the MGV and DASH, many units are designing their own homegrown systems, and very few of these systems are interoperable. The XVIII, III, and I Corps all have different systems using different software and communications protocols. All have to go through some type of gateway to talk with one another. The problem is even greater in that each division in III Corps has a different system. The 1st Infantry Division uses Microsoft Mail with a Windows for Workgroups Network Operating System (NOS), 4th Infantry Division uses ccMail with a Novell network. The 1st Cavalry Division uses NETLAN for messaging and for their NOS,[7] and the 2nd Armored Division recently implemented Windows for Workgroups.[8] Even in the Pentagon, there are numerous sub-networks that use different software but cannot communicate with each other.[9] The DMS will combine the two functionalities of AUTODIN and E-mail, will provide greater services, and eliminate the interoperability problems experienced today.[10]

The objective of the DMS program is for all users on the battlefield to have one system for writer to reader messaging that is capable of sending and receiving messages from the battlefield to the

White House. This service will eventually be extended to users below the maneuver brigade via the Tactical Internet, but probably not until well into the twenty-first century. This is largely dependent on future developments of transport and switching technologies and the network's ability to support an X.400 messaging capability at echelons lower than brigade command posts and separate battalions. This thesis will focus on the impact of transitioning from the existing Tactical Record Traffic System to a messaging system circa 2000. The primary focus is writer to reader messaging at the sensitive but unclassified (SBU) to secret level for those units that normally receive MSE support, that is, to the brigade and separate battalion level.

Assumptions

There are several controversial questions whose answers could have a major impact on the DMS transition strategy and therefore, the impact on DTLOMS. The following are six of the critical questions and the assumptions this thesis will make:

What Will The Army Do On The Battlefield?

As stated earlier, tactical planners are far behind strategic planners when it comes to DMS. Many people have many different ideas of how the Army should extend and implement DMS on the battlefield. The Army does not have one rock-solid plan free from errors. What the Army does have is a semiformal document developed by the Signal Center and USAISC that dictates a proposed architecture and transition strategy. This thesis assumes the Army will transition the existing messaging systems to the tactical DMS in accordance with the existing transition strategy.

To What Level Is DMS Extended?

The overall objective is to extend DMS to every weapons platform on the battlefield. During the Task Force XXI exercise in April 1997, the Army will digitize a complete brigade from the 4th Infantry Division (M). This Brigade will deploy to the National Training Center (NTC) to test various technologies. One of these technologies is the implementation of the tactical internet. The tactical internet will provide the maneuver forces with the equipment to transfer data horizontally and vertically across the battlefield. The goal is to provide situational awareness for all warfighters.

Although this is the objective, the Army will not be able to extend DMS that low for quite some time. This thesis assumes that in the near term the Army will only extend DMS to those users normally supported by an MSE switch, that is, to brigade and separate battalion headquarters.

What Are the Effects of, or on, Related Programs?

DMS affects, or is affected by, many other programs. An example is the Common Hardware/Software Program (CHS2). The purpose of CHS2 is to provide common platforms for all Army Tactical Command and Control Systems (ATCCS) and the Global Command and Control System (GCCS). This contract was held up in litigation resulting in a significant fielding delay. This thesis will assume that the CHS2 platforms are fielded. There are other systems that are similarly critical to the DMS program. This thesis also assumes these systems are fielded according to the timelines imposed by the program executive offices (PEO) and program managers (Pm).

What Protocols Will the Army Use?

The DMS is based primarily on the communications protocols X.400 and X.500. Both the current and previous Assistant Secretary of Defense for Command Control Communications and Intelligence (ASDC3I) mandated that all messaging would transition to the DMS based on these protocols.[11] This thesis assumes the Army will transition to X.400/500 in accordance with the mandates specified by the ASDC3I. This thesis further assumes that the encryption and security services required will come from the NSA MISSI program, also mandated by the current ASDC3I.[12]

What Is the Availability of Security Products?

The DMS and MISSI programs are separate programs yet are very dependent on each other. As stated earlier, the DMS must use MISSI products to provide warfighters the MLS capabilities referenced in the Enterprise Strategy. Simply put, the Army cannot do DMS without MISSI. MISSI security products will be fielded incrementally beginning this year and extending out through at least the next decade. In the past, timelines for MISSI products have shifted several years. A critical assumption of this thesis is MISSI security products will be available in the time periods currently briefed by the NSA customer advocacy team.

What Services Will the DMS Contract Provide the Army?

In May 1995, Loral Corporation was awarded a $496 million contract to provide DMS to all users whether home based, traveling, or tactically deployed. The impact on DTLOMS will be greatly determined by the system Loral delivers. An important assumption is that the messaging system the Army receives satisfies the basic requirements the DMS system is based on. The primary authority document for DMS is the Multicommand Required Operational Capability (MROC) 3-88. MROC 3-88 identified thirteen requirements that the DMS must satisfy.[13] This thesis assumes that Loral will deliver a system that meets the following thirteen requirements:[14]

Connectivity/Interoperability. The DMS will allow users to communicate with any other user within the DMS community. The community of users includes organizations and personnel of the Department of Defense. In addition, the DMS will support interfaces to systems of other government agencies, allies, and defense contractors. Connectivity will extend from writer-to-reader. Messages will be composed, accepted for delivery, and delivered as close to the user as practical.

Guaranteed Delivery/Accountability. The DMS will, with a high degree of certainty, deliver a message to the intended recipient(s). If the system cannot deliver a message, a method of promptly notifying the sender of the failed delivery must be available.

Timely Delivery. The DMS will recognize messages that require preferential handling. The urgency of the most critical information, especially for the warfighting forces, requires handling above and beyond simple priority.

Confidentiality/Security. Confidentiality precludes access to or release of information to unauthorized recipients. The DMS will process and protect all unclassified, classified and other sensitive message traffic at all levels and compartments.

Sender Authentication. The DMS will unambiguously verify that information marked as originating at a given source did, in fact, originate there.

Integrity. Information received must be the same as information sent. If authorized by the writer, the DMS may make minimal format changes to accommodate differences in capabilities between the component systems serving the writer and the reader. However, the DMS will ensure that information content of a message is not changed.

Survivability. The DMS will provide a service as survivable as the user it serves. It will not degrade the survivability of systems interfaced to it. Surviving segments of the DMS will be capable of reconstitution.

Availability/Reliability.

The DMS will provide users with message service on a continuous basis. The required availability of the DMS will be achieved by a combination of highly reliable and readily maintainable components, thoroughly tested software, and necessary operational procedures.

Ease of Use. The DMS will be flexible and responsive enough to allow user operation without extensive training. Use of the DMS will not require the knowledge of a communications specialist.

Identification of Recipients. The sender will be able to unambiguously identify to the DMS the intended recipient organizations or individuals. The necessary directories and their authenticity are part of the DMS.

Message Preparation Support. The DMS will support user friendly preparation of messages for transmission to include services, such as US Message Text Format (USMTF) assistance.

Storage and Retrieval Support. The DMS will support storing messages after delivery to allow retrieval for such purposes as readdressal, retransmission, and automated message handling functions, such as archiving and analysis.

Distribution Determination and Delivery. For organizational message traffic, the DMS will determine the destination(s) of each message and effect delivery in accordance with the requirements of the recipient organization. For individual message traffic, the DMS will effect delivery of each message to the individual(s) specified by the originator.

Endnotes

[1]Director of Information Systems for Command, Control, Communications and Computers (C4), Army Enterprise Strategy The Vision (Washington DC: Government Printing Office, 1993), Inside Cover.

[2]Ibid., 4.

[3]U.S. Army Information Systems Command, Defense Message System - Army (DMS Army) Tactical Architecture and Transition Strategy (Draft) (Fort Huachuca, AZ: 30 September 1994), ix.

[4]Ibid.

[5]Ibid., 10.

[6] U.S. Army Signal Center, Voice/Data Contention Study (Fort Gordon, GA: Directorate of Combat Developments 1991).

[7]U.S. Army Information Systems Command, Defense Message System - Army (DMS Army) Tactical Architecture and Transition Strategy (Draft), 10.

[8]This information was gathered prior to the recent III Corps restructure.

[9]Fed de Gastyne, Interview: Emmitt Paige, Jr. Talks About DMS, Insight Magazine, 1995, 2.

[10]Director of Combat Developments, Tactical Army Defense Message System Architecture and Transition Strategy White Paper, (Fort Gordon, GA: Signal Center, 1995), 1.

[11]Assistant Secretary of Defense for Command, Control, Communications and Intelligence, Memorandum for Secretaries of the Military Departments, Directors of the Defense agencies, and the Joint Staff, Subject: Electronic Mail Policy (Washington DC: 9 March 1995).

[12] Ibid.

[13]Director of Information Systems for Command, Control, Communications and Computers (C4), Multicommand Required Operational Capability 3-88, (Washington D. C.: Government Printing Office, 1988).

[14]Director of Information Systems for Command, Control, Communications and Computers (C4), Required Operational Messaging Characteristics, (Washington D. C.: Government Printing Office, 1988). 7.

CHAPTER 2

DEFINITIONS OF KEY TERMS

Like many other Army programs, DMS is full of acronyms, technical jargon, and a fleet of new equipment. It is important for readers to understand some of the key terms and key equipment, as well as who operates it and who pays for it. The following terms are critical to understanding this thesis. This thesis will define some of the key terms and key DMS components in alphabetical order.

Administrative Directory User Agent (ADUA). The ADUA is a software application that will allow the maintainers and infrastructure providers (Signal Corps) to manage the address directory.[1] Most E-mail users are aware of the user look up function. The ADUA is the software application that the Signal Corps will use to manage the DMS directory that essentially provides similar user look up functions. It is only a software application and will most likely run on the same platform as the Message Transfer Agent (MTA) and Directory System Agent (DSA). Both of these functions are defined below. DISA will buy all ADUAs.

Certification Authority Workstation (CAW). The CAW is a PC based application designed to program and manage the MISSI Fortezza and Crypto Cards (described under security products below). The CAW programs users Personal Identification Numbers (PINs), security keys, and the user's messaging privileges onto the Fortezza and Crypto Cards.[2] The CAW also performs directory and security management tasks. One planning option calls for the CAW to be integrated with the Army Key Management System (AKMS) and further integrated into the ISYSCON. NSA is researching the feasibility of this option for technical considerations and the SIGCEN is looking at MOS manning considerations. DISA will buy an undetermined initial quantity. Subsequent to the initial quantity the user will be responsible for purchasing the CAW.

Crypto Card. Crypto Card is similar in form and application to the Fortezza card described below. The security services of the Crypto Card are more robust and will allow messaging at the secret level. It is backward compatible with the Fortezza card and will be available around late FY 97.[3] The Major Commands (MACOMS) are responsible for purchasing and operating the Crypto Card.

Defense Message System. The DMS is the overall system that replaces the way we do both formal and informal messaging today. It consists of all hardware, software, procedures, standards, facilities, training, support and personnel used to exchange messages electronically between organizations and between individuals in the DOD.[4] The current subsystems of the DMS are AUTODIN and E-mail. DMS components are broken into two categories. They are either infrastructure, or user components.

Defense Message System Infrastructure Components. Infrastructure components are those pieces of hardware and software normally installed on the wide area network. These new components will have minimal effect on the average user. These components will, however, be installed somewhere on the MSE and TRITAC backbones and will most likely be integrated into the existing systems. The DMS infrastructure components are defined throughout this chapter. They are: message transfer agents, directory system agents, mail list agents, guards, multifunctional interpreters, certification authority workstations, and management workstations.

Defense Message System User Components. User components are those pieces of hardware and software normally installed, operated and maintained at the user workstation or on the Local Area Network (LAN). These components will have an impact on the user and the planners and managers as well. The user components are: user agent, directory user agent, Personal Computer Memory Card International Association (PCMCIA) card readers (from this point on this thesis will refer to PCMCIA cards as smart cards and therefore, smart card readers).

Directory System Agent (DSA). The DSA is a directory for users to access the address and public keys of other users. It works very similar to the user look-up function found in most E-mail applications used today. It also performs many of the same functions performed by the Tactical Name Server (TNS) in Node Center and TTC-39D packet switches. The following is an example of how it is used. If a tactical user wants to send a message to a user in the sustaining base, he will first access and then query the closest DSA for the sustaining base user's address and security key. If the local DSA has the information it will return it to the requester immediately. If not, that DSA will electronically search other DSAs for the information requested. Once the tactical user has the sustaining base users address and public key he can now address and encrypt the message. The Signal Corps will operate and maintain the DSAs and DISA will buy them.

Directory User Agent (DUA). The DUA is a software application that provides directory services and is collocated with the user agent on the users platform.[5] This is the software that allows users to look up other users in the network. Users are responsible for purchasing and operating the DUAs.

Fortezza. Fortezza provides security services for sensitive but unclassified (SBU) mail. It is a thick credit card sized card that is inserted in a standard smart card reader. The smart card reader can either be built into the platform or in an external reader. The card provides the user's Personal Identification Number (PIN), digital signature, private key, and various other information unique to that user.[6] The Fortezza cards and readers are considered user components and will be purchased by users.

Guards. Most everyone who uses E-mail today is familiar with the term "firewall". The purpose of a firewall is to protect one community of users from other hostile users. The MISSI version of the firewall is the Secure Network Server (SNS) which typically resides at the boundary between networks of different security classifications. The Army runs a secret high network and has a requirement to pass large quantities of data into the Nonclassified Internet Protocol Router Network (NIPRNET). To accomplish this, we must place an SNS between the two networks. The SNS plays an integral role in the DMS transition strategy and is the first of all the components to be given to the warfighter. The responsibility for operation and purchasing the SNS is under controversy.

Mail List Agent (MLA). The MLA performs mail list expansion for collectively addressed messages in a way similar to the AUTODIN Indicator Groups (AIGs).[7] In other words, the MLA allows a user to send one message to the MLA, and the MLA will send the message to the intended recipients. Again, the Signal Corps will maintain the MLA and DISA will buy them.

Management Workstation (MWS). The MWS provides the capability to manage DMS products and messaging services. Each MWS will allow remote monitoring and control of all DMS products. Currently, the MWS software will reside on a scaleable HP 700 series workstation and will be employed at Signal Brigade and Battalion Operations Centers.[8] Integration of the MWS function into the Integrated System Control (ISYSCON) is being researched by the Program Manager for Joint Tactical Communications Systems (PMJTACS). Again, the Signal Corps will maintain and DISA will buy the MWS.[9]

Message Store (MS). The message store is like an E-mail box. When a User Agent is down, relocating, or not operational, the MS receives messages from the MTA and holds them for later call up by the UA. Every MS can be configured to provide services such as automatic alert notifications for high precedence messages and automatic message forwarding based on certain criteria, such as message precedence.[10] The user is responsible for purchasing and maintaining the MS.

Message Transfer Agents (MTA). The MTA provides mail host services to local users and switching services for the infrastructure messaging network.[11] When a message is ready for transmission, it is signed and encrypted prior to transmission to the MTA. The MTA delivers messages to all addressed users. In the tactical environment MTA's will reside at all Signal Brigade and Battalion backbone and extension switchboards. The current transition plan has the MTA residing on a stand-alone platform and terminated off a LAN segment extending from backbone tactical switchboards. The Army eventually plans to integrate the MTA into the Enhanced Switch Operators Position (ESOP). Signal soldiers will maintain the MTA and DISA will buy them.

Multifunction Interpreter (MFI). During the transition period many users will still be dependent upon AUTODIN and Simple Mail Transfer Protocol (SMTP) e-mail systems, while others have migrated to the DMS X.400 system.[12] The MFI is the component that allows DMS users to interoperate while some users are still on AUTODIN, some are using other protocols, and some have transitioned to the DMS protocols. The Signal Corps will operate the MFI and DISA will buy them.

Multilevel Information System Security Initiative (MISSI). MISSI is an NSA initiative. The purpose of MISSI is to provide a set of products that can be used to construct secure computer networks in support of a wide variety of missions.[13] The primary MISSI customer is the DMS, where MISSI is used to support secure messaging.

MISSI Security Components. Security products are categorized as workstation, network, or guard products. Fortezza and Crypto Card are the primary workstation products this theses will address. This thesis will also briefly address another MISSI product called Secure Computing Workstation.

Multilevel Security (MLS). MLS is an essential enabling technology for the integration of various networked automated information systems into an effective global command and control system. MLS permits the integration of systems which contain information at different sensitivity levels by protecting against unauthorized information modification and disclosure; and, allowing system and information access only to users with proper credentials.[14]

Network Products. Network products typically reside at the boundary between local and wide area networks and provide highly robust encryption and access control services. Network products normally are used to encrypt an entire enclave of users. FORTEZZA cards only protect a single user. There is some controversy as to who operates and pays for network encryption products.

Secure Computing Workstation. This is NSA product used to be called the Trusted Workstation and prior to that APPLIQUE. The Secure Computing Workstation consists of a Crypto Card and security monitor software and will convert COTS workstations into trusted computing devices. It will allow a single workstation to process information spanning a security level range of unclassified through top secret.

User Agent (UA). The X.400 UA is the software that allows a user to perform DMS messaging and will function on the CHS2 platform. Since the UA is on the warfighter platform (MCS, AFATDS, etc.) the user is responsible for maintaining it. Users are also responsible for purchasing UAs.

Writer to Reader. Writer to reader simply means that one individual or organization writes the message and another organization or individual reads the message. There are no middle men. This also holds true for the security functions. The writer encrypts the message and the reader decrypts the message. Today that same message would travel through many hands and many telecommunications facilities.

Endnotes

[1]Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Systems, The Defense Message System Target Architecture and Implementation Strategy, (Washington DC: Government Printing Office, 1993), 3-9.

[2]Defense Information Systems Agency, DMS Capstone Material Fielding/Implementation Plan, (Washington, DC: Government Printing Office, 1995), 5. (cited hereafter as DISA)

[3]DISA, MISSI Implementation Plan, (Washington, DC: Government Printing Office, 1994), 7.

[4]DISA, Defense Message System Implementation Plan, (Ft. Huachuca, AZ: Government Printing Office, 1994), 2.

[5]DISA, Capstone Material Fielding/Implementation Plan, 4.

[6]DISA, MISSI Implementation Plan, 6.

[7]DISA, Capstone Material Fielding/Implementation Plan, 5.

[8]Ibid., 6.

[9]Director of Combat Developments, Tactical Army Defense Message System Architecture and Transition Strategy White Paper, (Fort Gordon, GA: Signal Center, 1995), 17.

[10]DISA, Capstone Material Fielding/Implementation Plan, 4.

[11]Ibid.

[12]Ibid., 5.

[13]DISA, MISSI Implementation Plan, xi.

[14]National Security Agency, Multilevel Information Systems Security Initiative (Ft. Meade, MA: Information Systems Security Office, 1995), 1.

CHAPTER 3

IMPLEMENTATION

As mentioned in chapter one, the Signal Center, along with USAISC, NSA, and other agencies developed a strategy for transitioning the existing Tactical Record Traffic System to the Tactical Defense Message System. It is important for all Signal leaders, information support planners, and information providers to gain a general understanding of this plan. Almost anything and everything that happens during this transition will have some impact on either one or more of the DTLOMS.

Again, this thesis assumes that the Army will transition in accordance with this plan. This chapter will briefly review the current messaging systems, some of the Band-Aids and quick fixes, the objective DMS system, and the three phases of the Army transition strategy. Chapter four will assess the impact across the DTLOMS spectrum.

Army Baseline Tactical Messaging Architecture

Today organizational and individual messaging is accomplished using one or a combination of the following three methods: AUTODIN via dedicated or dial-up circuits, Mobile Gateway Vans which provide e-mail through dial-up circuits into the circuit switching network, and Tactical EAC/Corps owned and operated proprietary E-mail systems using Simple Mail Transfer Protocol (SMTP).

Narrative message service in the current tactical environment is provided by the Tactical Record Traffic System (TRTS). Messages are either formal (JANAP 128, DOI 103) or informal such as nonformatted text, pictures maps etc. The Automatic Digital Network (AUTODIN) is the only provider of worldwide classified message services.[1]

Typically, tactical AUTODIN message services are provided by communications terminals connected to tactical message switches which are in turn connected to an AUTODIN Switching Center (ASC). There is no connectivity between the messaging system and the Tactical Packet Network (TPN) currently used by many units for data transfer between existing Command and Control (C2) platforms such as the Maneuver Control System (MCS), the All Source Analysis System (ASAS), the Advanced Field Artillery Tactical Data System (AFATDS) and the Standard Theater Army Command and Control System (STACCS). Figure 3 represents the Army's baseline messaging architecture.

Army Objective DMS Architecture

Initially, DMS will be extended to those users currently supported by a tactical switchboard via a LAN segment. Thus, DMS support will be provided down to brigade command posts and separate battalions within the division.

Objectively, DMS will be extended to all tactical users from the National Command Authorities to the Sergeant in an M1 tank. All tactical users will have one system for writer-to-reader messaging on an unclassified, information support backbone using one multifunctional, secure computing workstation that is merely an extension of the Defense Information System Network.[2]

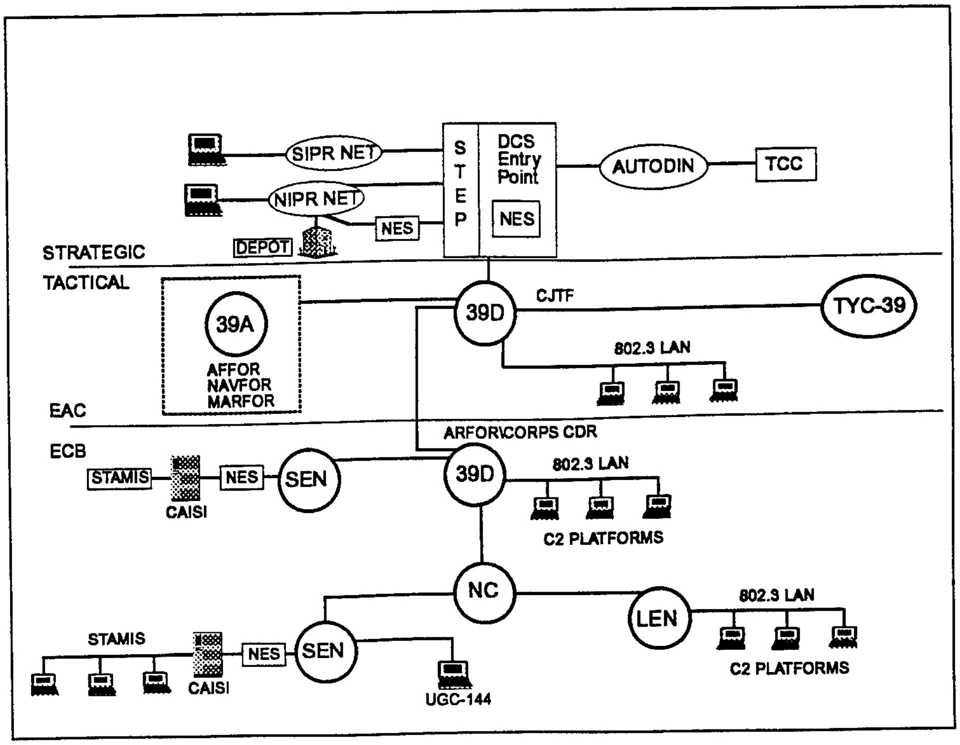

Figure 3. Baseline Architecture

This service will eventually be extended to users below the maneuver brigade via the tactical internet for both organizational and individual messaging. This is largely dependent, though, on future development of transport and switching technologies and the network's ability to support an X.400 messaging capability at echelons lower than brigade command posts and separate battalions.

In the strategic and sustaining base environments, Nonclassified Internet Protocol Router Network (NIPRNET), the Secret IP Router Network (SIPRNET), and the Joint Warrior Intelligence Communications System (JWICS) will all become the Defense Information Systems Network (DISN). Users on the DISN, whether homebased, traveling or tactically deployed, have some type of security device at their workstation which will enable them to draft, send, and receive messages of all classifications anywhere within DISN. Tactical Packet Network (TPN) users, using Common Hardware and Software (CHS) equipment and an NSA approved workstation security device will have the ability to do the same. Figure 4 depicts the objective Tactical DMS Messaging Architecture.

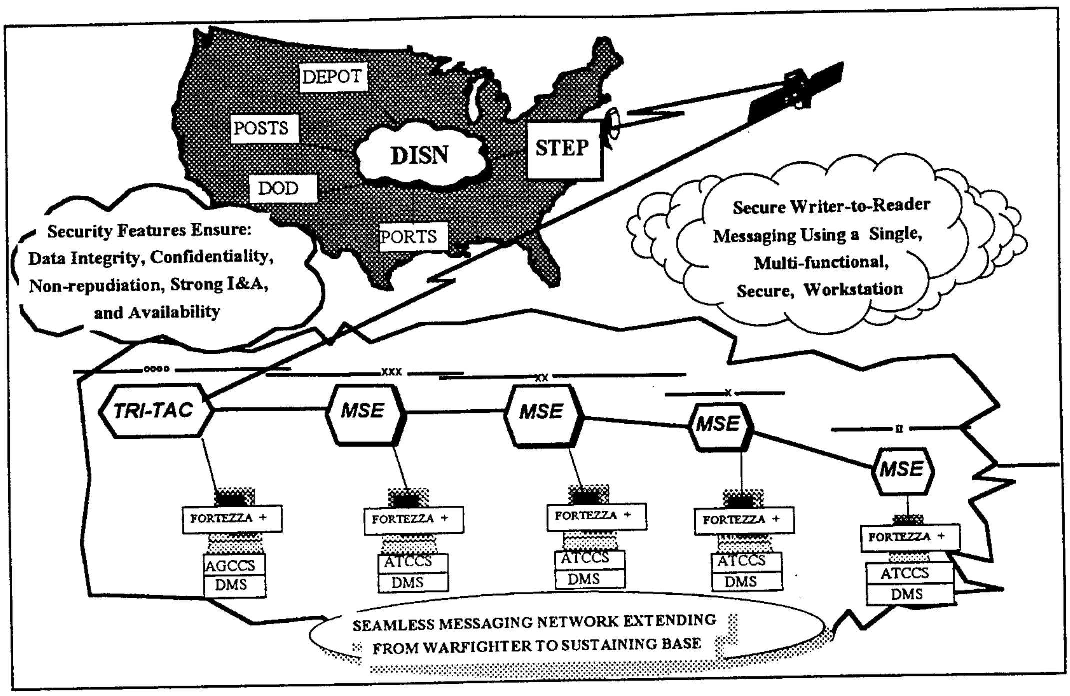

Figure 4. Objective Architecture

Very Near Term Architecture

Warfighters want a more efficient means to command and control their forces. Division and Corps Commanders today will not wait until the year 2000 or even 1997 for the existing programs to provide them the tools. They are, in fact, spending large amounts of money testing and buying Commercial Off The Shelf (COTS) products to facilitate their desire to move information around cheaper and faster than they can today. The Signal Center, USAISC, DISC4 and several other agencies, are well aware of this and are working overtime to provide various quick fixes until the programmed equipment arrives. This thesis will briefly explain some of the current products being tested and used by warfighters in the field.

The current message switch (TYC-39) is very large, costly, manpower intensive and very difficult to deploy. The TYC-39 in total consists of four, five-ton trucks with shelters, and three trailers. The crew consists of six soldiers.[3]

The Signal Center is currently testing a much smaller switch called a CGS-100. The basic CGS-100 is nothing more than a hardened platform that provides store-forward message switching and a link between the formal AUTODIN messaging system and the Tactical Packet Network (TPN). This is significant for both signal and maneuver commanders especially when planning for initial messaging capability during force projection operations. The Battle Command Battle Lab (BCBL) at Fort Gordon, Georgia has conducted significant testing of the CGS-100 both in the lab as well as in the field at Fort Bragg and Fort Hood.

Products that enable the warfighter to move large amounts of other than command and control (STAMIS community) data from the battlefield to the sustaining base via the tactical packet network are also available. Some of these products only provide bulk data transfers and are not in the purest sense considered messaging.[4] They do, however, require some discussion so the reader has an understanding of how these communities of users are, or could be, supported.

The first product is a network layer encryptor called the Network Encryption System (NES). NES was tested during several Joint Warrior Information Demonstration Networks (JWIDS) and recently underwent limited user test and fielding at Fort Bragg, Fort Hood, and other locations[5]. These systems are currently used to cryptographically separate the unclassified Standard Army Management Information Systems from the "secret high" command and control community. A NES is located between the Combat Service Support Automated Information Systems Interface (CAISI) and the Small Extension Node (SEN) Switch. Another is located somewhere in a strategic or sustaining base location, perhaps at the Standardized Tactical Entry Point (STEP). NES allows users to essentially tunnel through the TPN to move large unclassified files to the sustaining base.

The next promising product is an early, non-DMS compliant version of the Secure Network Server (SNS). Headquarters, Pacific Command is currently using the SNS as a guard between a secret and unclassified local area network. The Army has a similar requirement to connect the secret TPN to the unclassified NIPRNET. The current version of the SNS would allow the Warfighter to send and receive SMTP, ASCII Text E-mail from the TPN to and from the NIPRNET.[6] This SNS can be upgraded to version four, the first DMS compliant SNS. Using a loaner SNS from NSA, SIGCEN conducted testing at the Fort Gordon Battle Lab, and a follow-on user assessment at Fort Riley, Kansas.[7] The test proved that the SNS could provide TPN to NIPRNET, text only, services, and was deemed a success. The early version SNS will be used as a transitional component in 1996 to provide E-mail to the battlefield until DMS is implemented.

Army Near-Term Architecture (1997-1998)

Tactical messaging will continue to be largely SMTP-based during this time, however, traffic processed via AUTODIN will begin migration to DMS as products are fielded. There will be significant changes to the tactical architecture and thus a significant impact on the DTLOMS. The Army will take several steps during the near term to begin the transition to a tactical DMS. These steps will enable tactical users to communicate with users on the NIPRNET using the initial MISSI products to provide security for sensitive but unclassified level messages, and will prepare the tactical messaging systems for the transition to DMS X.400.

The first step is the augmentation of the current Message Transfer Agent (MTA) and Tactical Name Server (TNS) in backbone and force projection switches with fully functional X.400 Intermediate Message Transfer Agents (IMTAs), X.500 DSAs, and Message Stores (MS). These DMS functions will be installed on a single, stand-alone platform on a 802.3 LAN segment in the TTC-39D, Node Center Switch (NCS) and TTC-50 Forced Entry Switches (FES). Message transfer agents and directory system agents are considered DMS infrastructure components, and as such, will be provided and funded by DISA.

Designated TPN users will be provided a Fortezza smart card, a card reader and X.400 DMS User Agent (UA) software. Fortezza will enable TPN users to access both the NIPR and SIPR Nets from the tactical packet network. Users desiring to send messages to users on NIPRNET would choose to invoke the security privileges embedded in the Fortezza card. Users desiring to send messages within the tactical packet network and to SIPRNET would simply choose not to invoke Fortezza since they would be sending messages between two secret networks. Classified and Special Compartmented Information users will continue using AUTODIN and their current systems (Trojan Spirit). STAMIS and other SBU communities would continue to use NES.

The Fortezza compatible E-mail software, Fortezza cards, and smart card readers are considered user components and will be funded and implemented by the Major Commands. The exact costs are not yet known but some cost figures are $350.00-$400.000 for the entire package depending on the type card reader. In accordance with a mandate signed by the ASDC3I, all personal computers and command and control workstations procured from January, 1995 forward should be capable of supporting at least two smart card slots.[8] Therefore, the need to provide external card readers to tactical users will initially be high, but should decrease as components are replaced and card readers are redistributed.

Another major step during this phase is the installation of the version four Secure Network Server (SNS) in all Standardized Tactical Entry Points (STEPS) and other designated reach-back points. Users who had previously installed the SNS during the very near term would simply upgrade their current SNS to the version four SNS. This SNS is the first DMS compliant version. Version four will support X.400 mail, X.500 directory, and security services provided by MISSI. This SNS restricts messaging into and out of the TPN/NIPRNET to authorized users and messages which meet security criteria by invoking a number of pre-configured filters. A feature of this SNS includes Fortezza digital signature which provides authentication, non-repudiation, and integrity.

The Army will also place Multifunction Interpreters (MFIs) at the standardized tactical entry points and signal brigade and battalion operations centers. Not everyone will immediately transition to X.400, so the need for an interpreter to convert data formats will initially be high. A Multifunctional Interpreter (MFI) is a DMS transitionary component used for protocol and format conversion and will enable user interoperability between AUTODIN, SMTP, and DMS X.400.

The Fortezza card must be programmed and managed. This is done by the Certification Authority Workstation (CAW). The CAW programs contain features such as level of classification authorized and private key, and provides the users electronic signature. NSA is investigating the feasibility of porting the CAW software to the Automated Key Management System (AKMS), with the intent of integrating security services to a single platform.

Accomplishing these actions will provide tactical users the ability to send formal, organizational messages to users on the NIPR and SIPR Nets and will provide limited interoperability with non-DMS capable users. The STAMIS systems and other sensitive but unclassified users will continue using NES to tunnel through the TPN to NIPRNET. Top Secret and Special Compartmented Information users will continue to use legacy systems to protect their message traffic between the TPN and the JWICS. Figure 5 depicts the Tactical DMS Near-Term architecture.

Army Midterm Architecture (1998 - 2000)

During this time period, DMS products and services will become common throughout the strategic and sustaining base

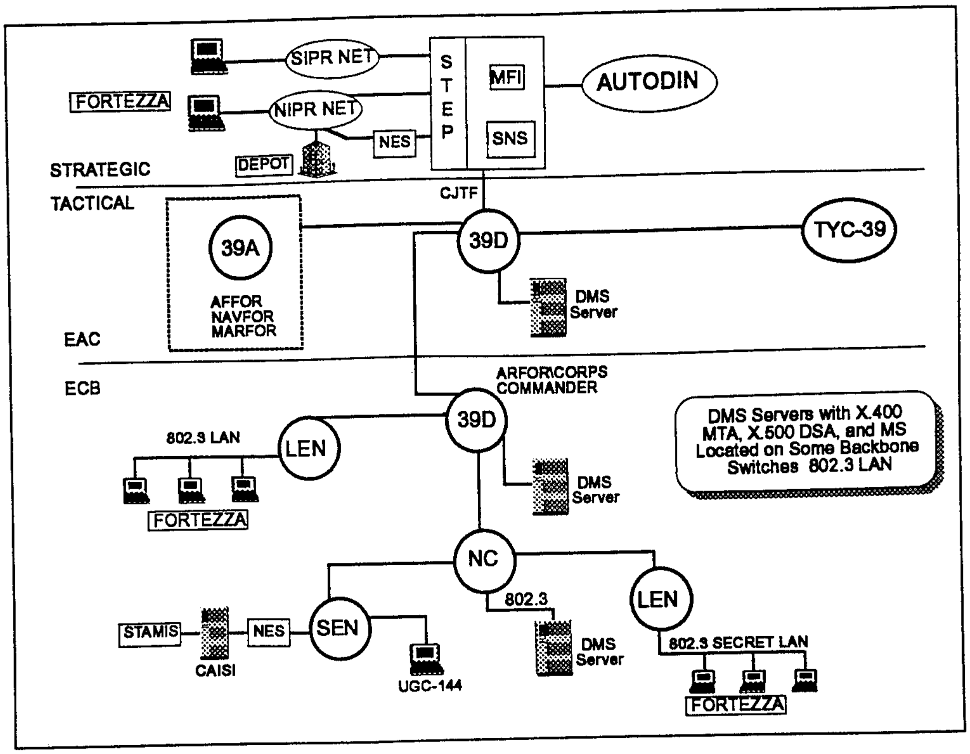

Figure 5. Near Term Architecture

environments. To ensure the implementation of a single, seamless system, the tactical environment will continue to undergo several changes to make DMS common throughout the battlefield. AUTODIN components will still be used for messaging, but use will be limited and will decrease in preparation for the planned closing of the network in the year 2000.[9] The following actions will enable tactical users to communicate with the sustaining base and each other using X.400 based components with MISSI security products.

One of the first actions during this period is to integrate the X.400 MTA, X.500 DSA and the Message Store on all backbone and Forced Entry Switches' Enhanced Switch Operations Position (ESOP) Sun SPARC 20 platform. Integration of these and other DMS components with the ESOP platform is a very necessary action. DMS components do not come with the personnel resources to operate and maintain them. Nor does the Army want to increase airlift requirements because of the extra platforms that the DMS program initially brings. ESOP is a funded program that will provide a more robust, user friendly platform for switch operators. As such, it is a logical platform to port some of the DMS infrastructure functions. The Tactical Name Server will remain during this phase to support Legacy e-mail systems requiring it.

The Army will continue fielding of DMS UA software to tactical users. This will include all remaining Army Tactical Command and Control Systems and Global Command and Control Systems user platforms. User agents reside on user owned and operated workstations and provide most of the user interface functions such as message preparation support, staffing, message release, and distribution determination and delivery.

The Army will now field the Crypto Card (second version of Fortezza) to tactical users as required. Crypto Card (formerly Fortezza +) is a workstation security product similar in form and application to Fortezza. The security services are the same except that Crypto Card provides stronger signature and hash algorithms.[10] Crypto Card will be backward compatible with Fortezza, but once available, the Army will no longer be able to use Fortezza to secure data at the secret level. Thus, upon NSA approval, Fortezza will only be used to process secret as an interim solution until Crypto Card is available. It should be available for purchase sometime in 1998. Crypto Card compatible UAs, cards, and card readers are considered user costs and will be funded and implemented by MACOMS. As stated earlier, the total cost per workstation will initially be between $350.00 and $400.00.

Another change in the security architecture will see the network encryption system used for STAMIS and SBU communities replaced with a tactical guard. The tactical guard will provide these communities with a write-up capability to users located on the secret TPN. It will also provide users serviced by the secret tactical packet network, Combat Service Support C2 Systems for example, the capability to write down to STAMIS and SBU communities. Additionally, the tactical guard will enable STAMIS and SBU communities to draw necessary DMS support from the same infrastructure that supports TPN users. Tactical guards will be located and installed at all Node Center Switches (NCS), Large Extension Node Switches (LENS), and Small Extension Node Switches (SENS).

The network encryption systems no longer used for STAMIS and SBU communities will be re-utilized on local area network segments supporting TS and SCI communities. Once AUTODIN shuts down, DMS support to TS and SCI users will have to be a swivel-chair operation. Users on the secret TPN will have to send and receive messages to TS and SCI users on a like secret system. The TS and SCI operators will then have to take the information from the secret system, and manually input it into the TS and SCI system for further transmission. This issue is discussed further in chapter four.

During this phase, the Army will not be able to provide infrastructure support, necessary for use of the DMS, on the same local area network segment supporting TS and SCI operations. If the Army must provide DMS infrastructure support to TS and SCI users, they must do so on a separate local area network segment. Figure 6 depicts the tactical DMS mid-term architecture.

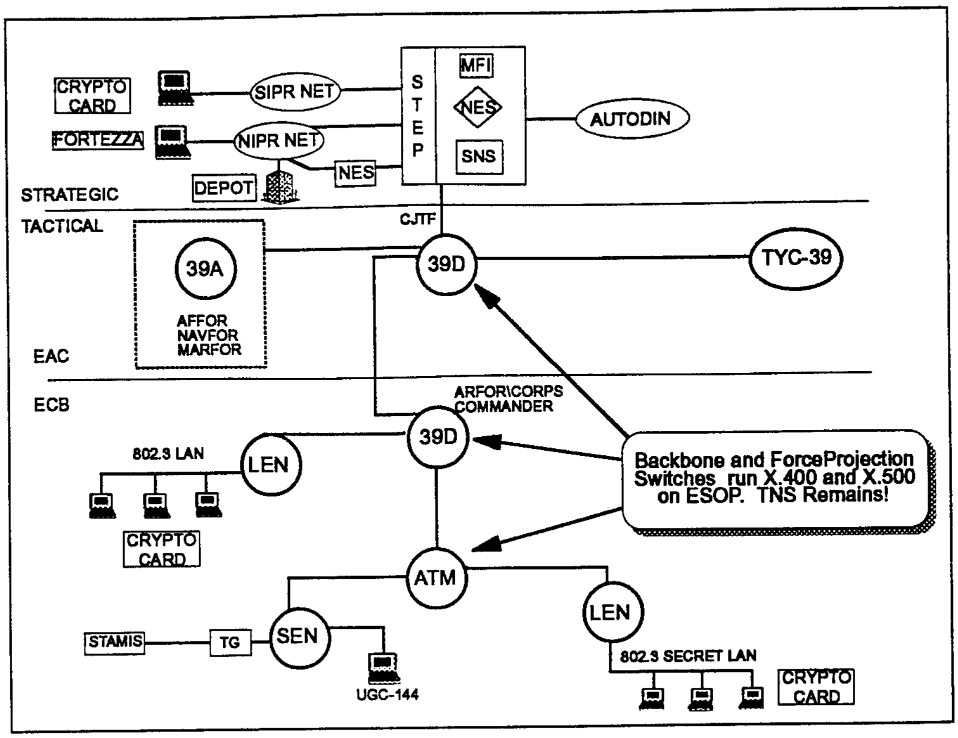

Figure 6. Mid Term Architecture

Army Far-Term Architecture (2000+)

For most warfighters this is several years away. As stated earlier, commanders want to know what the combat developers and acquisition community can do today. This is, however, important to signal planners and maneuver users because of the vast changes not only to the DMS network, but the entire tactical communications system.

During this timeframe we will see our tactical transmission and switching systems transition to high capacity trunk radio systems, Asynchronous Transfer Mode (ATM) switching systems, and Integrated Services Data Network (ISDN) based switching systems.[11] These technologies will significantly increase the velocity and throughput of all data services. The Army will also experience increased demands for numerous data and video services over tactical systems. This is very significant because the increased performance in the Army's tactical transport systems may enable the implementation of DMS services in echelons below the brigade command post and separate battalion. This will have to be investigated once the Army has assessed the DMS performance and its impact on the tactical systems.

The following actions could be completed to allow users with a TS and SCI requirement access to a sustaining base system like JWICS via the area ATM and ISDN switching systems.

Multilevel Information Systems Security Initiative release 3 (Secure Computing Workstation, formerly Trusted Workstation and prior to that APPLIQUÉ) could be fielded to designated users around the year 2003. This release will enable conversion of COTS workstations to trusted computing devices. This secure workstation consists of a crypto card and security monitor software. The security monitor software effectively turns an untrusted COTS workstation into a multilevel security workstation. This permits a single workstation to process information spanning a security level range of unclassified through top secret. Additionally, this workstation will be interoperable with Fortezza and Crypto Card.

The next step will be to port the X.400 message transfer agent and the X.500 directory system agent software to the data server located at all ATM hub switches. The tactical name server will no longer be used. Figure 7 illustrates the potential Army far term architecture.

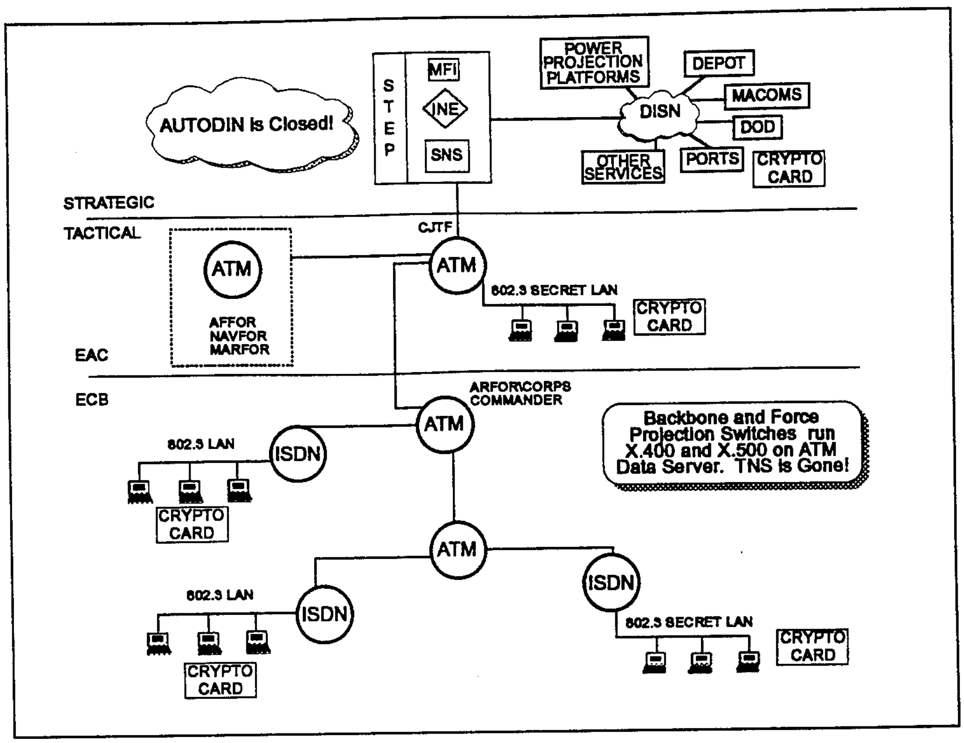

Figure 7. Far Term Architecture

The matrix shown in Figure 8 captures the overall strategy for transitioning from each of the near, mid, and far term implementation phases as depicted in earlier paragraphs of this chapter. The matrix also serves to show the relationship and dependence that DMS and its associated components have on other programs and efforts focusing on transport systems and multilevel security. As stated in chapter 1, this transition strategy assumes that the time lines of both DMS and other programs remain on track, and that initiatives such as the integration of DMS components into switching and network management programs also remain on track.

TIME LINE	TRANSPORT	DMS USERS	MANAGEMENT	BACKBONE	MULTILEVEL SECURITY	INTEROPER-ABILITY
	Transmission & Switching	DMS UA	MWS	MTA, DSA, MLA, MS	CAW, SNS, INE	MFI
NEAR 97-98	Most users on TPN. Some dial-in	UGC-144/MCS replaced with CHS2 TCU & LCU	-MWS: Stand-Alone on CHS1 Platform @ SCC/CSCE	-Components: Stand -Alone @ Sig Bde/Bn Ops & TRITAC/NCS/ FES	-SNS @ STEP, Sig Bde/Bn Ops -CAW @ G-6, Sig Bde/Bn Ops -Fortezza: SBU-SBU capability -NES: CAISI/STAMIS users	Stand-Alone @ -STEP -SCC/CSCE
MID 98 - 2000	All users on TPN	Complete fielding for all organizations	-MWS integrated into ISYSCON on SUN platform	-MTA/DSA/MS integrated with ESOP	-T.G. @ SEN/LEN: STAMIS/SBU -SNS @ STEP, Sig Bde/Bn Ops -CAW @ G-6, BSO, Sig Bde/Bn Ops -Fortezza +: SBU-Secret capability -NES: Reused for INTEL TS/SCI	Stand -Alone @ -STEP -ISYSCON
FAR 2000 +	DISN Colorless	All Org. and individuals fielded to Bde and Sep Battalion	JCPMS ISYSCON	-ATM Hub Switch	-T.G. @ ISDN Switch: STAMIS/SBU -CAW/AKMS combined @ Bde ISYSCON, G6, Sig Bde/Bn S3 -INE: INTEL TS/SCI users	-STEP -Integrated with selected tactical switches

Figure 8. Transition Matrix

Endnotes

[1]U.S. Army Information Systems Command, Defense Message System - Army (DMS Army) Tactical Architecture and Transition Strategy (Draft), (Fort Huachuca, AZ.: 30 September 1994), 5.

[2]Director of Combat Developments, Tactical Army Defense Message System Architecture and Transition Strategy White Paper, (Fort Gordon Georgia: Signal Center, 1995), 20.

[3]U.S. Army Information Systems Command, Defense Message System - Army (DMS Army) Tactical Architecture and Transition Strategy (Draft), 5.

[4]Director of Combat Developments, Tactical Army Defense Message System Architecture and Transition Strategy White Paper, 24.

[5]Ibid., 24.

[6]Ibid., 25.

[7]Ibid., 25.

[8]Assistant Secretary of Defense, Command, Control, Communications and Intelligence, Memorandum for Secretaries of the Military Departments, Directors of the Defense Agencies, Directors of the DOD Field Activities, Director, Joint Staff, Subject: PCMCIA Card Slots in Personal Computer and Workstation Contracts, (Washington DC: Government Printing Office, 1994).

[9]Director of Combat Developments, Tactical Army Defense Message System Architecture and Transition Strategy White Paper, 28.

[10]Defense Information Systems Agency, MISSI Implementation Plan, (Washington, DC: Government Printing Office, 1994), 7.

[11]Tony Loop, Warfighter Information Network and the Next Generation of Switches Using ATM Hub and ISDN White Paper, (Fort Gordon GA: Directorate of Combat Developments, 1995).

CHAPTER 4

ANALYSIS

The extension of the Defense Message System to the battlefield will fill a much needed void in the area of tactical communications. As the Army transitions to a CONUS based, force projection Army, the need for interoperability between the deployed force and the sustaining base will increase exponentially. Commanders, running split-based operations, must have the capability to pass data from places like Bosnia, Somalia, and Haiti to places like Fort Bragg, Fort Hood, and the Pentagon.

DMS will significantly enhance the tactical commanders' capabilities. Conversely, there will be a number of impacts created by this system that will affect the entire doctrine, training, leader development, organization, material, and soldier (DTLOMS) spectrum. This chapter will describe the impact of extending DMS to the battlefield on each area of the DTLOMS.

Impact on Doctrine

Of all the DTLOMS, the extension of DMS to the battlefield will have the largest impact on doctrine and material. Material impacts are for the most part quantifiable, but are in many cases not assessable until the Army develops the doctrine for tactical DMS.

Signal support doctrine must be developed to support the fielding, installation, operation, maintenance, security and management of the DMS system in the tactical environment. Who will be provided the service? At what classification? How often will they use it? How much bandwidth will it require? Who will manage the system? How many management and other infrastructure components does the Army require? Where are they located and who operates them? What policies govern the DMS system? Today the Army cannot answer any of these doctrinal questions.

As mentioned in chapter 1, the Army Enterprise Strategy is based on 10 principles designed to ensure the future warfighter's ability to maintain information superiority over any opponent.[1]

Based on these principles, the Enterprise General Officer Steering Committee chose eleven tasks as the first step in implementing the strategy.[2] Task one is: Using the existing Integrated Battlefield Architecture (IBA) as an operational C4I requirements baseline, the Director of Information Systems for Command Control Communications, and Computers (DISC4), with TRADOC as its combat developer lead, will sponsor a study to determine the feasibility of expanding the scope of the IBA into a more comprehensive Operational Architecture (OA).[3] In simple terms, the OA will tell the Army who talks to whom, over what type of system, how often, and with what type of data. DMS must be considered when developing this architecture.

The OA is critical to the extension of DMS to the battlefield because today, there is no doctrine that determines who gets DMS. Current Operational Facility (OPFAC) rules clearly state who receives phones, faxes, MCS, ASAS, etc. Those units who are already extending E-mail type services to the battlefield are doing so without a Basis Of Issue Plan (BOIP).

A major reason this is so critical is that there are physical limitations to the Army's tactical packet network. It is difficult to predict the impact DMS will have on the network or what portion of the limited bandwidth the DMS system will require. The US Army Signal Center at Fort Gordon, Georgia has a Network Assessment Model (NAM) that is designed to answer these type of questions. The Signal Center cannot, however, model the system until they know the number of users they are dealing with.

Task two of the Enterprise Strategy is to develop a Technical Architecture (TA). The TA will ensure interoperability between tactical, strategic, and sustaining base Army and joint information systems. It is a set of standards that are applicable to information processing, data transport, information standards, and human computer interfaces. The standards defined in the TA establish the framework for achieving interoperability and commonality among hardware and software on the digital battlefield.[4]

All DMS components will be developed in accordance with the TA. This open systems architecture makes maximum use of commonly accepted commercial standards and protocols, and should solve the interoperability problems experienced today.

The final doctrinal task in the Enterprise Strategy is to develop a Systems Architecture (SA). The SA shows the specific hardware and software needed to provide the connectivity required in the operational architecture. Both architectures are very closely linked. The SA is a description of the physical location and connectivity of an information system, which includes: identification of all equipment (MTAs, DSAs, CAWs, etc.), and its physical deployment; the specifications of parameters such as the bandwidth required or available on each circuit; and the description, including graphics, of technical characteristics and interconnection of all parts of an information system.[5]

The Army must develop a systems architecture that includes the components of the DMS system. The US Army Communications Electronic Command (CECOM) Research, Development and Engineering Center (RDEC), as the system engineer and the US Army Signal Center, as the user representative, will jointly develop this architecture with assistance from other TRADOC schools and various program managers.

The operational, technical and system architectures are critical to the successful implementation of DMS on the battlefield. The operational architecture will tell the DMS planners who messages with whom, how often, sending what type of data and at what security classification. The technical architecture will ensure interoperability of all DMS components, and the systems architecture will provide a blueprint of the infrastructure to connect it all together.

Doctrine must dictate the level of classification authorized by duty position. Some planners believe that all users require a multilevel secure system capable of transmitting and receiving messages from unclassified through top secret. Although this is the goal, it is not feasible, realistic or even needed for the majority of users. The tactical packet network operates at the secret level. This means that all data, even if it is unclassified, is classified at the secret level. The majority of the Army's command and control systems from MCS to AFATDS to GCCS will all be connected to the TPN and, therefore, are secret systems. Very few users require the ability to send anything above the secret level. There will, however, be times when certain users will require the ability to send a top secret message. Those users must be identified in the operational architecture as well.

This impacts mainly on the Certification Authority (CA). The CA is the person responsible for managing and programming the smart cards via the Certification Authority Workstation. This person must know what level of message each user is authorized to send in order to prevent abuse of the system. A Battalion S3 may think he is important enough to have the authority to release a top secret message, and he may be. The point is that neither he nor the CA should be in the position to make that call. Doctrine should clearly tell him.

The frequency of DMS messaging is difficult to quantify since there is no historical data. In the past, planners were able to accurately predict the amount of messaging traffic given upcoming events. During Desert Storm, the 93rd Signal Brigade provided communications support to the VII Corps. Narrative message traffic was used extensively as a means of communications and initially, the network was capable of handling the load. There were, however, times that the network bogged down and messages were backed up by the thousands. A significant lesson learned was that messaging traffic must be managed to prevent a total collapse of the network.[6] The NAM must be able to model and assess DMS messaging at its peak to accurately assess its impact. Once the network assessment is done, doctrine must be developed to specify which users have priority during peak times.

Management of any large computer network is a demanding, complex task. The computer systems that will be running DMS will be geographically dispersed, linked by multiple communications means, and frequently relocated. Currently, there is no doctrine that determines who will manage the DMS system. The Signal Corps must be given the overall responsibility of managing all DMS WAN or infrastruture components. Further, these management functions and systems should be integrated into the Army's Integrated Systems Control (ISYSCON) program.

The ISYSCON is another Army program designed to deliver a single, integrated system capable of managing a multitude of communications systems. Doctrine must determine who and where the management systems and functions will be located and it must be developed quickly. It may already be too late to integrate the DMS management function into the ISYSCON. If it is, the Army must develop an entirely different, stovepipe management system just for the DMS application.

Policies governing the security of DMS messages are an essential doctrinal component of DMS. To facilitate the development of this doctrine, the Defense Information Systems Agency established a Security Policy Working Group (SPWG). The SPWG has already set up a DMS security policy framework which outlines policies and plans to support the DMS program. This framework defines standard communications security terminology, identifies existing policies and architectures that apply to the DMS; outlines new policies and architectures that are needed specifically for the DMS; defines classes of messages handled by the DMS, and also defines the security services that may be appropriate for each class; outlines the process by which the DMS and its elements are technically evaluated with regard to their security features and safeguards, and by which they are approved to operate, and identifies DMS security officials and their responsibilities.[7] Within this framework, the following will be developed:

Security Classification Guide. This will specify how to classify, reclassify, declassify, and otherwise handle DMS messages.[8]

Basic Security Policy. This document will identify the minimum security safeguards that are required for operation of the DMS and its facilities and components, and for subscriber participation in the system.[9]

Component Security Standard. This will regulate the life cycle of a DMS physical component from a security standpoint. This standard will set uniform, general guidance that will apply to all components and their functions, to all organizations that deal with the components, and to all facilities and activities that house them. The standard will include guidance for computer security evaluation criteria and clearance levels.[10]

These documents do not currently specifically address tactical DMS users because the DMS is designed to be a single messaging system that will support users whether homebased, traveling or tactically deployed.[11] However, operations at homebase and the battlefield are different and will require the SPWG to address these differences.

One example is the smart card. When a user at Fort Bragg has to update his Personal Identification Number (PIN) he simply goes to his certification authority who, via the certification authority workstation, updates his card. A user on the battlefield may be located at the Brigade Tactical Operations Center and his certification authority may be in the Division Support Area. He may not have the time, transportation; or the tactical situation may not allow him to drive to the DSA to get his PIN updated. The SPWG must address this and other unique tactical issues, and must develop policies that address them.

Currently, only DA civilians are voting members of the SPWG. Tactical communications providers and users must be integrated into the SPWG and must identify and develop policy for the unique tactical security issues.

The Army must solve the doctrinal issues quickly. As stated in chapter three, some of the DMS products are already in use in the tactical environment and many more are programmed for the very near future. The Defense Information Systems Agency must identify the agencies responsible for developing doctrine and must then provide them the resources to quickly develop and publish it.

Impact on Training

Training will also be significantly impacted by the extension of DMS to the battlefield. Today, all personnel in the Army are potential users of an automated system, and this potential increases daily as more automated systems are fielded. Eventually, all Army personnel will be potential users of the DMS system.

Recent Advanced Warfighting Experiments (AWEs) revealed that U.S. military tactics and training are beginning to lag behind the pace of technological advances on the battlefield.[12] As a consequence, the Training and Doctrine Command (TRADOC) feels that because the majority of soldiers are not trained to fully exploit military systems being developed for the Army's digitized battlefield, many computer skills should be taught as routinely as combat skills.[13]

This section will examine the existing automation training provided by TRADOC institutions, the training that will be provided by LORAL, and some unresolved DMS training issues.

Signal soldiers and other information providers receive the majority of their automation skills through institutional training. Institutional training is training conducted at TRADOC or other DOD schools. It is generally individual skill oriented training, although many of those skills may support the execution of collective tasks or missions.[14]

Officer training at the Signal Center is available for Signal Officers and officers of other branches. The training includes conference or small group instruction on many automation issues, equipment and systems. Automation training for officers at the Signal Center also requires hands-on operator efficiency to interface with local E-mail systems and the Defense Data Network, and the ability to install and troubleshoot local area networks. Signal Officer training is expanding as the planning and managing of automated joint information systems becomes the Signal Officer's primary technical duty.[15]

Automation training for Signal Officers begins in their Signal Officer Basic Course with more than 60 hours of classroom and hands-on instruction. The Signal Officer Advanced Course continues that training a few years later with over 110 hours of automation training including instruction on data communications, Local Area Network installation and management, and the TPN. Officers in the branch detail program attend a branch qualification course that includes 54 hours of automation training.[16]

Signal Warrant Officers require many automation skills, and their institutional training is intense. MOS 251A (Data Processing Technician) Warrant Officers receive 469 hours of automation training at their Basic Course and 304 hours at their Advanced Course. The other Signal Warrant Officers receive 108 hours of automation training in their Basic Course and over 90 hours in their Advanced Course.[17]

Officers from other branches as well as signal officers may attend automation courses at the Computer Science School (CSS) at Fort Gordon, Ga. The CSS offers 15 automation functional courses, including UNIX System Administration and Software Engineering Fundamentals. The Branch Automation Officer Course is an eight week, 320 hour course that trains officers from all branches in computer hardware, software, data communications networking and information security.[18]

Officer training at some TRADOC schools follows the Fort Gordon model closely. At others, automation training for officers is minimal. All officer Basic and Advanced Courses do provide automation training which goes beyond just operating the unit's or section's PC. Officers require and receive limited training on their specific Battlefield Automation System (BAS) that supports them, such as the Maneuver Control System (MCS).[19]

At the Signal Center, Noncommissioned Officers receive training in a variety of automation tasks. At the Advanced Noncommissioned Officers Course (ANCOC), automation training for each of the signal Career Management Fields (CMF) varies. CMF 25 receives 41 hours of computer literacy training. CMF 29 gets 172 hours, CMF 31 gets 120 hours and CMF 74 receives more than 221 hours. The CMF 74 course includes training on software engineering, artificial intelligence and use of specific automated systems. Basic Noncommissioned Officer Course (BNCOC) students at the signal center receive between 40 hours and 199 hours of automation training according to their MOS. Other training centers are beginning to introduce automation training to their programs of instruction for BNCOC and ANCOC.[20]

Finally, institutional automation training for enlisted soldiers is primarily presented in Advanced Individual Training (AIT) at a TRADOC school. Some signal MOSs require extensive automation skills such as 74D, Computer Systems Operator, or 39G, Automated Communications Computer Systems Repairer. Most AIT automation training is specific to the automation skill required.[21]

It is not yet clear what type of training will be provided by LORAL. The DMS Request For Proposal (RFP) Statement Of Work (SOW) requires them to furnish, conduct, and maintain Commercial Off The Shelf (COTS) or contractor modified COTS training courses for users, operating system administrators, message handling system administrators, directory system administrators, management work station managers, and government instructors for each type of training offered. The instructor course materials must also be provided for reproduction and use within the DOD.[22] The contractor is required to provide classroom training and also self taught (computer based or video tape based) courses. This thesis assumes that LORAL will provide these courses. The courses are as follows:

Basic User Training Course. This course will introduce user agent product users, regardless of technical ability, to the concept of military messaging and the role of the user agent product. Upon completion of this course, users should be able to understand and use all of the features of the messaging system.[23]

Operating System Administrator Course. This course will include operating system initialization, operation, troubleshooting, upgrading, and security procedures for the hardware platforms offered on the contract.[24]

DMS Message Handling System Administrator Course. This course will teach DMS MHS system administrators, as a minimum, system, initialization, operation, troubleshooting, upgrading, access control, and security procedures for interfacing with other systems, restart/recovery, degraded mode operations, and shutdown procedures.[25]

DMS Directory System Administrator Course. This course will teach the DMS directory system administrators, at a minimum, system initialization, operation, troubleshooting, upgrading, access control and security procedures for interfacing with other systems, restart/recovery, degraded mode operations, and shutdown procedures.[26]

Management Workstation System Product Course. This course will teach messaging system managers to use and operate the MWS products in order to perform the management of messaging and directory components. This course will provide the MWS operators with the ability to identify messaging problems reported by the MW, to perform the proper actions to isolate and further define these problems, to take necessary actions to circumvent these problems, and to take necessary actions to correct these problems. This course will also provide the MWS managers with the ability to perform the other management functions of configuration, fault, performance, security, and accounting management.[27]

The statement of work does not specifically address training for tactical DMS users for the same reason that existing DMS doctrine does not. The ASDC3I has clearly stated that he does not want a separate system for tactical users.[28] The Army must, however, ensure that its unique training requirements are addressed.

The basic user training course may be sufficient for the majority of the Army's tactical end users. These users will only see DMS as another application on their existing command and control platform, so their training requirements will be minimal. The contractor will most likely provide this training as part of a New Equipment Training (NET) package.

The Army must then institutionalize DMS user training by providing instruction in all Advanced Individual Training (AIT), noncommissioned officer, and commissioned officer training courses. This includes the basic and advanced noncommissioned officer courses, and the officer basic and advanced courses. This is not only for the Signal Corps. All branches of the Army will run DMS on their Battlefield Functional Area (BFA) Army Tactical Command and Control System (ATCCS). These are user owned, operated, and maintained systems. All branches of the Army must institutionalize the user training package.

The operating system administrator, message handling system administrator, directory system administrator, and management course must also be institutionalized. They could be incorporated into existing courses such as the training course required for all functional area 53 officers, and the current systems administrator course taught at Fort Gordon, Georgia. Prior to any of this, doctrine must identify the soldiers responsible for these functions.

The most significant training issue is the training required for those soldiers who will operate the infrastructure components. Specifically, the message transfer agent, directory service agent, and administrative directory user agent. As stated in chapter three, these functions will initially be performed on a local area network located at some backbone switches, but will later be integrated into the Enhanced Switch Operators Position.

Simply sending a NET team to Fort Gordon to train a few soldiers will not work. These functions will be integrated into a platform currently used to program and manage the circuit and packet switched networks. Soldiers receive their institutional training on these systems during their AIT at Fort Gordon, Georgia. All DMS products must be integrated not only into the ESOP in the field, but the platforms in the schoolhouse as well.

It is more than just a simple software load. Instructors at Fort Gordon will have to be trained and portions of the training curriculum will have to be rewritten. New training materials must be developed and all equipment used for training must be upgraded in accordance with any upgrades to equipment in tactical units.

Fort Gordon, Georgia must be the nerve center for all Army tactical DMS training. The Air Force is the Executive Agent (EA) for DMS and has recently proposed conducting all DMS training at Maxwell Air Force Base. This will not work for Army tactical installers, operators, maintainers and managers. The Signal Corps will perform these functions, so it only makes sense to provide training for these functions at the Signal Center.

Impact on Leader Development

The DMS, in itself, does not significantly impact leader development. DMS is just one piece of the incredible digitization of the battlefield. DMS, when combined with other automation functions and leader responsibilities, will significantly affect leader development not only in the Signal Corps, but across other branches as well.

This is not just a Signal Corps responsibility. As mentioned above in training, the ATCCS systems such as MCS, AFATDS, CSSCS, FAADC3I, and ASAS are user owned and operated systems. These systems, with all their applications to include DMS, will place additional responsibilities on many leaders at different levels. Field Manual 24-7, Army Battle Command System (ABCS), Systems Management Techniques dictate some of these responsibilities.

An example is the responsibilities of the S3 or G3. FM 24-7 says that he is responsible for integrating the five ATCCS systems to support the tactical mission. He accomplishes this by: planning, integrating, and employing ATCCS; planning and monitoring sustainment training; and developing the ATCCS annex to the OPORD. Terminal operators and staff users are responsible for: installing, operating, and maintaining assigned hardware and software; interfacing their equipment with tactical communications (the Signal Corps WAN), and implementing security policies and procedures. A final example is the responsibilities of the staff elements. They are: operating terminals in garrison and tactical environments in accordance with appropriate manuals and standard operating procedures, maintaining trained personnel to operate the terminals, organizing and controlling distribution of information, and developing and implementing internal standard operating procedures for assigned terminals.[29] The point here is that DMS, as well as the other applications running on the ATCCS systems, will impact more than just the leader development of the Signal Corps.

More than ever, Signal Corps officers must be able to blend sound leadership skills with technical proficiency to provide the information systems required to project, sustain and protect America's forces, and win our nation's wars.[30] To accomplish this mission, the Signal Corps has two interrelated subfields in which officers develop: Signal Operations and Systems Engineering.

Signal operations officers lead signal platoons and command companies, battalions and brigades providing signal support for division, corps, and theater level operations worldwide. They serve as executive officers, operations officers and in many other staff positions in every Signal unit.[31]

Within combat arms units, such as infantry battalions or artillery brigades, signal operations officers supervise the planning, employment and operation of tactical Signal equipment and systems. They ensure voice and data communications within the unit and connectivity to networks of higher, lower and adjacent units.[32]

Systems engineers are the Army's formally trained information systems engineers. They apply information technology theory and systems engineering principles to real-world Army requirements. There primary job is to plan and manage the integration and interconnection of diverse types of Signal equipment and systems into interoperable local area and wide area information networks supporting division, corps and theater level operations[33].

As stated above, other staff elements and branches of service have significant responsibilities for automation. The user owned and operated concept does not, however, relieve the Signal Corps of the overall responsibility of providing communication support to the fighters. FM 24-7 also clearly dictates the roles and responsibilities of the G6 or supporting Signal Officer (SIGO). The G6/SIGO is responsible to the operations officer for the establishment and maintenance of ATCCS communications links by: linking geographically separated command posts through the WAN, maintaining the communications network in the face of tactical movement, battle damage and equipment failures; monitoring the WAN performance, maximizing the throughput capability of the WAN, coordinating troubleshooting, enforcing procedures to ensure consistency and compatibility of the ATCCS connections to communications systems, and overseeing the planning and installation of LAN configuration procedures.[34]

The responsibilities of tactical DMS, and a multitude of other current and future automation systems will quickly make the traditional leader development system obsolete. The line between signal operations and signal engineering is already blurry and will soon be gone. Signal officers of the twenty first century must be both operators and engineers.

Impact on Organizations

The overall impact on organizations will most likely be minimal. This is difficult to assess, though, without the DMS doctrine referenced earlier. It is relatively safe to say that the Army will at a minimum, require the number of personnel currently required to provide messaging for the Tactical Record Traffic System (TRTS). The Signal Center submitted 11 requirements to DISA that are unique to tactical DMS. One of them is that the tactical DMS system must be supportable within the existing force structure.[35] The messaging system must not require additional manpower. Nor should it require significantly greater skills to operate, use, or manage.

One of the primary goals of DMS is to reduce cost and staffing levels. By implementing DMS the tactical Army will surely reduce messaging costs, but it cannot afford to reduce staffing levels. Soldiers will still be required to install, operate, maintain, and manage the DMS components.

There are currently thirty four AN/TYC-39 Tactical Message Switches in the Army inventory. Each is manned by six soldiers for a total of 204 personnel currently providing the WAN services for the tactical record traffic system. The Signal Corps and the Army must fight to keep these slots as they will be needed to perform other DMS messaging functions.

As stated in chapter 3, the MTA, DSA and other functions will eventually be incorporated into the ESOP. During the near term, however, these functions will be provided somewhere on a LAN connected to one or more of the backbone switches. Someone will be required to operate the MTA and DSA during this timeframe. Further, soldiers have not been identified to run the management workstation or the certification workstation. Some of the current message system providers (the 204 soldiers) could be retrained to perform these functions.

Chapter 3 also mentions that the TS/SCI community of users will have to perform a swivel-chair operation to send secret data into the TS/SCI data network. This may or may not require additional soldiers. The intelligence community must take a close look at this issue when determining the impact of DMS on their force structure.

A final issue is the availability of computer systems experts at the officer level. DMS, along with many other digitization efforts, may require an officer to perform automation management functions across all battlefield functional areas. There are two ways the Army could facilitate this. First, the Signal Corps could change its leadership development structure as previously stated under leader development. All Signal Corps officers could be trained as both operators and engineers. This would significantly lengthen the basic and advanced courses. Another possible solution is to provide a functional area 54 officer at each unit from battalion up. This would significantly impact all branches because, while they are serving in this capacity, they would not be able to serve in their respective branches.

The Signal Center, along with TRADOC, is currently studying this issue. Solving it may be difficult but is necessary and critical to the overall effort to digitize the battlefield.

Impact on Material

A common thought in the DMS planning community is that DMS is nothing more than an application layer program that will run on any command and control system. The DMS User Agent (UA) and Directory User Agent (DUA) are software applications, but there are many infrastructure systems required to run them. Unlike doctrine, most of the material impacts are obvious and easily quantifiable. The magnitude of many of these changes depends, however, on the doctrine developed for DMS. This section will analyze the impact on bandwidth and some of the major material related issues.

Bandwidth, and the Army's lack of it is one of the hottest topics in any C4I discussion. It is a hot topic because it is limited and everyone is competing for it. Users want video teleconferencing, telemedicine, total asset visibility, situational awareness, real time imagery etc. All of these require large amounts of bandwidth and currently the Army does not have it.

The TPN provides 64 Kb between backbone switches and only 16 Kb from the backbone switches to the extension switches. The Army is not yet sure what the impact of extending DMS to the battlefield will be. What the Army does know is that the X.500 and X.400 protocols that DMS uses will require more bandwidth than the existing protocols used on the TPN today.

General Telephone and Electric (GTE) Government Systems Communications Systems Division conducted a DMS and TPN interoperability study in December, 1994.[36] Their preliminary studies found that the overall increase on the tactical backbone due to an X.400/X.500 upgrade is expected to be no greater than fifteen to twenty percent. The exact number is dependent on a number of factors to include MTA distribution, DSA distribution, and the X.400 Elements Of Service (EOS) used.[37]

One of the primary factors in the increase in bandwidth required is the additional overhead due to Directory Access Protocol (DAP). This is the protocol used in the directory user agents. Using DAP will require two hundred to two hundred fifty percent more bandwidth than that currently used by TNS registration and query messages. Assuming that DSAs are only located at backbone switches, this will cause a problem on extension links which support larger user communities.[38]

Fortunately, the Internet community has a similar problem and is already developing a fix for it. This problem can be eliminated using a protocol under development by the internet community called Connectionless Lightweight Directory Access Protocol (CLDAP) in lieu of DAP. GTE's study reports that by using this protocol there would be no increase in traffic due to user interactions with the directory. This protocol is expected to reach maturity by the 1997 timeframe.[39]

The DMS protocols X.400 and X.500 have generated a great deal of concern because of their increased use of bandwidth. There is, however, another major concern with the X.500 protocol.

As stated in chapter three, X.500 will replace the existing Tactical Name Service (TNS) sometime during the midterm phase of the transition. To be an effective messaging system that supports the warfighter, DMS X.500 directory services must support the user as he enters, relocates within, and leaves the theater of operations. The current TNS provides a Reverse Address Resolution Protocol (RARP) capability which enables a tactical user to affiliate and reaffiliate with the messaging system after he has relocated from his previous physical location. This capability must also be supported by the DMS X.500 directory service.

As alluded to earlier, it will be very difficult to accurately assess the impact of DMS, and many other programs, until we complete some very important doctrine pieces. The operational and system architectures are critical to accurately assessing the bandwidth problems. The operational architecture will establish the doctrine for the end users, and the systems architecture will establish doctrine for connecting those users.

The impact of DMS components during the very near term will be minimal. There are some important considerations, however, that must be addressed. Implementation of the CGS-100, initial version of the Secure Network Server, and the Network Encryption System (NES) will all impact the end user and the Signal Corps to some degree.

The CGS-100 does not replace the TYC-39. It is a piece of messaging equipment that augments the TYC-39 during force projection operations. It is also more that just a single platform in a suitcase. To effectively operate it, the user needs several other pieces of equipment. The CGS-100 will require a printer, an uninterrupted power supply, secure telephones, link encryption devices, in some cases network encryption devices, and transit cases.

The NES used by the Combat Service Support (CSS) community is a network layer encryptor developed by Motorola Corporation. It is designed to encrypt the CSS data and essentially tunnel through the secret TPN. Past tests have proven its worth and several units are purchasing them and using them to great benefit. The issue is that there are many other network layer encryptors available that provide similar features and functions. Since the Technical Architecture is not formal yet, there is no way to ensure interoperability among these systems. It is very conceivable that CSS users at Fort Bragg are encrypted with an NES, and CSS users at Fort Monmouth are encrypted with GTE's Tactical End to End Encryption

Device (TEED). Both TEED and NES use different procedures to get to the same ends but do not interface with each other.

During the near term the primary issue is the integration of the X.400 MTA and X.500 DSA on the battlefield. The MTA and DSA will eventually be integrated into the ESOP. Initially, the Army will perform these functions on a LAN located at one or more of the NCSs. Both functions will operate on the same platform but it will be a different platform than currently used for circuit and packet switching functions. When the MTA and DSA migrate to the ESOP, these platforms can be utilized for other automation functions. The major issue is availability and funding of these platforms. It is not yet clear who pays for the platforms.

As stated earlier, the majority of users will see DMS as just another application running on their ATCCS or GCCS platform. The vehicle for purchasing the platforms for these systems is the Common Hardware Software Contract Second Version (CHS2). The initial statement of work for CHS2 did not require the vendors to provide internal PCMCIA Card readers. An Engineering Change Proposal (ECP) was submitted in the spring of 1995 specifically requesting internal PCMCIA slots. This is significant because the Army could potentially receive a half billion dollars worth of computers and have to buy external card readers for many of them. The card reader is considered a user component and would have to be purchased by the user at a cost of around two hundred dollars.

During the near term, selected users will receive the Fortezza card. This card was designed to secure data at the sensitive but unclassified level and the next release, Crypto Card, was to secure data at the secret level. Since Crypto Card will not be available for some time, NSA will allow users to secure data at the secret level using the Fortezza Card. Once Crypto Card is available, Fortezza will no longer be used for sending secret data. The impact of this is clearly cost, because many users will have to purchase two different smart cards. Each card will cost approximately one hundred dollars.

The Army must quickly decide whether or not to integrate the Certification Authority Workstation into the Electronic Key Management System(EKMS), or field an entirely different platform. The Army's version of the EKMS is the Army Key Management System (AKMS). Both the AKMS and CAW perform security functions such as key management, so it makes sense to integrate the two. The Signal Center initiated a request to NSA requesting just that. It is not yet clear whether or not NSA plans to integrate the two functions.

Similarly, the Army must quickly decide whether or not to integrate the DMS Management Workstation (MWS) functions and equipment into the ISYSCON. ISYSCON provides management functions for the tactical WAN and the DMS MWS provides management functions for the DMS WAN. Ideally, It would benefit the Army to integrate the DMS functions with an existing platform. If not, at a minimum the MWS must be located in the ISYSCON. Either way, planners must quickly resolve this issue before it's too late.

One way to solve the problem of commanders' appetites for bandwidth is to give them more. The Army plans to do that by eventually transitioning the existing switching systems to more efficient technologies like Asynchronous Transfer Mode (ATM) and Integrated Services Digital Network (ISDN) switching. The Army must begin planning for the integration of all DMS infrastructure products into these systems.

Impact on Soldiers

On the surface it appears the impact of extending DMS to the battlefield on the soldier will be minimal. The reality is, however, that the extension of DMS to the battlefield will have a significant impact on the soldier. Issues such as workload, additional training, and retraining must be addressed prior to implementing the DMS system on the battlefield.

If the DMS infrastructure components are integrated with current infrastructure components, then the Army will not require additional soldiers to operate, install, or maintain the DMS components. If the Army integrates the DMS MTA and DSA into the ESOP, the current switch operators will operate them. If the DMS MWS is integrated into the ISYSCON, the soldiers currently providing management functions will operate and manage it. If the CAW is integrated into the AKMS, the existing security managers will manage the security functions.

These initiatives will significantly increase the workload already imposed on these soldiers. The operators that administer the DSA and MTA on the ESOP already have a considerable workload. In addition to running the DMS components, they also must provide the switching services for the existing voice and data networks. They already manage voice databases and the TNS functions of the data network.

The imposition of the DSA and MTA may impose so great a workload that the operators cannot effectively provide the services of voice and data that are so critical to the warfighter's ability to command and control his forces. The same applies for those soldiers providing the management and security functions. As the Army digitizes and adds more automation systems, many soldiers will have less time to perform their primary skills.

If DMS components are integrated into existing systems, many soldiers will require additional training. As stated in chapter three, the Signal Center must serve as the center for all Army tactical DMS training. This means that the soldiers performing these functions will either have to return to Fort Gordon, Georgia for additional training, or a New Equipment Training (NET) team will have to go to them. This is very significant. There are currently 1,295 soldiers that provide the backbone or force projection switching services, and all of them will require the training. This does not include those soldiers that will require the security or management functions. New soldiers will receive this training during their AITs. The imposition of DMS will, however, increase the length of those AITs affected.

Some soldiers may have to be completely retrained and may even require an MOS change. As stated earlier, the Army must maintain the slots for the 204 soldiers already performing messaging services. All of these soldiers would have to be retrained to perform DMS type messaging services. Again, this could be accomplished at Fort Gordon, Georgia or by a mobile NET team. The Signal Center must first determine the most effective utilization of these soldiers.

Another of the Army's unique tactical requirements for DMS messaging is that the DMS messaging system must not impose such a degree of complexity and difficulty that soldiers cannot be easily trained to use or manage the system.[40] To the degree possible, the system must provide user friendly interfaces for both use and management. Messaging functions should take place in the background, as the tactical computer is running different operator applications. If this is what the Army receives off the contract, then the impact on those soldiers operating the ATCCS terminals should be minimal and the basic user training provided by the NET teams should be adequate.

Endnotes

[1]Director of Information Systems for Command, Control, Communications and Computers (C4), Army Enterprise Strategy The Vision, (Washington DC: Government Printing Office, 1993),

[2]Department of the Army, C4I Technical Architecture, (Washington DC: Government Printing Office, 1995), ES-2.

[3]Director of Information Systems for Command, Control, Communications, and Computers, Army Enterprise Strategy, (Washington DC: Government Printing Office, 1994), 4-2.

[4]Richard Volz, Tactical Internet for Task Force XXI White Paper, (Fort Gordon GA: Directorate of Combat Developments, 1995), 2.

[5]Ibid., 3.

[6]Department of the Army, 93rd Signal Brigade After Action Report for Operations Desert Shield and Desert Storm, (Germany: 93rd Signal Brigade, 1992).

[7]Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Systems, The Defense Message System Target Architecture and Implementation Strategy, (Washington DC: Government Printing Office, 1993), 4-14.

[8]Ibid.

[9]Ibid.

[10]Ibid., 4-15

[11]U.S. Army Information Systems Command, Defense Message System - Army (DMS Army) Tactical Architecture and Transition Strategy (Draft), (Fort Huachuca, AZ.: 30 September 1994), 1.

[12]Pat Cooper, "U.S. Army Strives to Close Tactics, Technology Gap." (Defense News, Volume 11, Number 5, 1996), 14.

[13]Ibid., 14.

[14]U.S. Army Computer Science School, FM 11-58 Draft, (FT. Gordon, GA. 1993), 6-2.

[15]Ibid., 6-6.

[16]Ibid.

[17]Ibid., 6-7.

[18]Ibid.

[19]Ibid.

[20]Ibid., 6-8.

[21]Ibid.

[22]Headquarters, Electronic Systems Center (AFMC), Request For Proposal (RFP) No. F01620-93-R-A211, Defense Message System (DMS) Government Open Systems Interconnection Profile (GOSIP) Acquisition Statement Of Work, (Hanscomb AFB, MA: Government Printing Office, 1994), 28.

[23]Ibid.

[24]Ibid.

[25]Ibid., 29.

[26]Ibid.

[27]Ibid.

[28]Assistant Secretary of Defense, Command, Control, Communications and Intelligence, Memorandum for Secretaries of the Military Departments, Directors of the Defense Agencies, Directors of the DOD Field Activities, Director, Joint Staff, Subject: Electronic Messaging Policy Implementation Guidance, (Washington DC: Government Printing Office, 1995).

[29]Headquarters, Department of the Army, Field Manual 24-7, Army Battle Command System (ABCS) Systems Management Techniques, (Washington DC: Government Printing Office, 1995), 2-4.

[30]U.S. Army Signal Center, Signal Corps Pamphlet, (Georgia: Fort Gordon, 1994), 3.

[31]Ibid., 8.

[32]Ibid.

[33]Ibid., 9.

[34]Headquarters, Department of the Army, Field Manual 24-7, Army Battle Command System (ABCS) Systems Management Techniques, 2-4.

[35]U.S. Army Information Systems Command, Defense Message System - Army (DMS Army) Tactical Architecture and Transition Strategy (Draft), 28.

[36]GTE Government Systems, Tactical Packet Network/Defense Messaging System Interoperability and Tactical Packet Network/Command Post Architecture Interconnectivity Study Report, (Massachusetts: GTE Communications Systems Division, 1995).

[37]Ibid., Executive Summary.

[38]Ibid., Executive Summary

[39]Ibid., Executive Summary.

[40]U.S. Army Information Systems Command, Defense Message System - Army (DMS Army) Tactical Architecture and Transition Strategy (Draft), 28.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

The DMS will significantly enhance the tactical commander's capabilities. Conversely, there will be a number of impacts created by this system that will affect the entire Doctrine, Training, Leader Development, Organization, Material, and Soldier (DTLOMS) spectrum.

Doctrine

There is currently no doctrine for the specific implementation of DMS in the tactical environment. Initially this was because tactical DMS users were not a part of the planning team. Later, this was intentional because the ASDC3I wanted to ensure that DMS was a single integrated system, not a separate system for users in garrison and users on the battlefield.

There are many issues and requirements unique to tactical users that must be addressed before extending the DMS system to the battlefield. Signal support doctrine must be developed to support the fielding, installation, operation, maintenance, security, and management of the DMS system in the tactical environment.

Tactical DMS doctrine must also be written and integrated into the operational, technical and systems architectures. Many of the questions posed in chapter 3, such as who is fielded DMS, how often and what type of messages are sent, location and number of infrastructure components, and the bandwidth required for messaging will be answered in the operational and systems architecture. The technical architecture will ensure interoperability between DMS and other automation components and applications.

Additionally, security and messaging policies must be written specifically for the tactical user. The tactical Army must ensure that it is well represented at any working groups or policy making board. The Army must further ensure that any policies or doctrine developed are supportable by the tactical user. Finally, the Defense Information Systems Agency, National Security Agency, and any other organization must consult with the Signal Center on any matters dealing with the extension of DMS to the battlefield.

Training

Like doctrine, there are no specific training packages designed for tactical users. Again, this is designed to ensure the Army fields one, integrated system. Planners must, however, develop specific training packages for the user at the actual terminal, the tactical infrastructure providers, the tactical WAN managers, and the tactical security managers.

Fort Gordon, Georgia, and the Signal Center, must assume executive agency for tactical DMS. Further, the Signal Center must be the focal point for DMS training. The Army cannot allow the Air Force to provide all tactical DMS training at Maxwell Air Force base.

The Army must further institutionalize DMS training at all training centers across all ranks. Sustainment training packages and embedded training aids must also be developed for the tactical user.

Leader Development

Leaders, specifically Signal Corps officers and FA 53 officers will be significantly affected by DMS and the multitude of other information systems. The Signal Corps must take a close look at realigning the current system for signal officer development and must erase the line currently separating signal operators from signal engineers.

As stated in chapter 4, the DMS system will be another application on the ATCCS system. Many other leaders will have significant responsibilities for the installation, operation, maintenance, and management of these systems. The Army must also determine the extent of leader development required for leaders other than signal officers or FA 53s.

Organizations

Tactical organizations may or may not see significant changes caused by the extension of DMS to the battlefield. At a minimum, the Army will require the same number of personnel currently required to provide messaging for the Tactical Record Traffic System. The tactical Army will not see a decrease in the amount of personnel required to install, operate, and maintain the DMS system. For this reason it is critical for the Army to retain the existing manpower slots.

The Army must determine who will operate each DMS component during each phase of the transition plan. The intelligence community must also determine if any additional soldiers are required to provide secret to top secret/special compartmented information message exchange. Finally, the Army must determine the number of automation experts required at the officer level.

Material

DMS is not just another application that will be integrated into the ATCCS. There are many impacts on the existing tactical infrastructure system both in terms of hardware and software. Combat developers and Program Managers must work closely together to ensure integration of like systems into the same platform. Examples of this are the ESOP and MTA/DSA, the AKMS and CAW, and the ISYSCON and MWS.

Once doctrine is developed, the Army must model the tactical DMS system to determine the actual impact on bandwidth. Some of the bandwidth studies do not indicate a significant increase in the amount of bandwidth required. High level planners must, however, remember that DMS is just one of the many new programs and applications competing for this very limited resource.

Soldiers

On the surface it appears the impact of extending DMS to the battlefield will be minimal. The reality is, however, that the extension of DMS to the battlefield will have a significant impact on the soldier.

The majority of DMS functions will most likely be integrated into other systems and will not require additional soldiers or MOSs to operate. They will, however, create a much greater workload on some already busy soldiers.

The DMS will also affect many soldiers because many will have to set aside their primary duties to receive additional training on the DMS components. This may occur on station, but they may also have to return to the Signal Center to receive the training. Additionally, many soldiers may have to be completely retrained and may even require a MOS change.

If the DOD is to have a single, integrated messaging system, they must, in finite detail, consider and address the issues and requirements that are unique to the tactical user and information systems providers. Once doctrine is developed, the Army must model the tactical DMS system to determine the overall feasibility of extending it to the battlefield, and its overall impact on doctrine, training, leader development, organizations, material and soldiers.

APPENDIX A

LITERATURE REVIEW

Many soldiers, sailors, airmen, marines, scientists, government civilians, and government contractors have spent countless hours discussing, writing, solving, testing, and studying almost every facet of the DMS program. DMS is not only an Army problem but transcends the joint and international boundaries. The Army has joint working groups, joint forums, service working groups and even international working groups. These professionals have produced many documents and conducted many tests with the ultimate goal of fielding a reliable, secure, state of the art messaging system. The majority of the documents and tests do not include the implementation of DMS in the tactical community of users. None assess the impact of extending DMS to the battlefield.

Many of these documents are listed in the bibliography, but a few of the more critical ones are described below. Previous efforts are categorized as orders, plans, doctrine, studies, or test results.

Orders include authority documents, requests for proposal, working group charters, and mandates from the Assistant Secretary of Defense for Command Control Communications, Computers, and Intelligence (ASDC3I).

Orders

ASDC3I Mandates

In October, 1992 the previous ASDC3I mandated that all electronic mail would migrate to DMS compliant X.400 and X.500 protocols.[1] In March, 1995, the current ASDC3I mandated the same.[2] On 7 July, 1994 the ASDC3I mandated that protection of all Department of Defense Sensitive But Unclassified (SBU) electronic mail is the minimum need the DOD must meet through the use of MISSI Release 1.0. He further mandated that all personal computers and workstations procured in the future shall be capable of supporting at least two Personal Computer Memory Card International Association (PCMCIA) cards of the Type II height configuration.[3]

DMS RFP

The DMS Request For Proposal (RFP) No. F01620-93-R-A211, Defense Message System (DMS) - Government Open Systems Interconnection Profile (DMS-GOSIP) Acquisition was written in very general terms and did not specifically require the vendors to demonstrate a Tactical DMS system. The original statement of work stated that tactical would be treated as a "pre-planned product improvement".[4] Change 1 to the RFP deleted that statement and said that DMS would be fielded as one complete system that would support the entire DMS community of users to include deployed tactical users.

MROC 3-88

The primary authority document for DMS is the Multicommand Required Operational Capability 3-88 (MROC 3-88) published by the Joint Chiefs of Staff in February 1989. MROC 3-88 defines thirteen primary requirements the DMS must satisfy. These requirements are very general and were patterned after the requirements from AUTODIN. Although the requirements delineated in MROC 3-88 also apply to TDMS, they do not take into consideration the unique tactical operational and implementation requirements.

ROMC

The Required Operational Messaging Characteristics (ROMC), a DISA document, was later developed to refine the high level MROC requirements into more specific, quantitative, or qualitative requirements. Again, the ROMC applies to TDMS but does not consider the operational and implementation requirements.

Plans include those documents that detail a specific event using specific resources during a specific time period. They also include concepts of operations and architectures.

Plans

DMS Army Tactical Architecture and Transition Strategy (Draft)

This document was developed by USAISC with help from the Directorate of Combat Developments, Fort Gordon, Ga. It is currently the only document that begins to describe the evolution of the Army's Tactical Record Traffic System to the Defense Message System. It describes the DMS-Army tactical transition from the baseline to the implementation of the objective architecture.

DMS Concept of Operations

The DMS CONOPS is a living document developed by USAISC under the direction of the ASDC3I. The CONOPS is available via the World Wide WEB (WWW) and is a "one stop shop" for DMS. The CONOPS defines and describes all components of the DMS program including hardware and software. It also describes functions and responsibilities of those soldiers and civilians who install, operate and maintain the DMS infrastructure components.

MISSI Implementation Guide

This plan was published in 1994 and was produced by the Defense Information Systems Agency Center for Information Systems Security at the direction of the ASDC3I. The purpose of this plan is to guide Service and Agency planners in implementing MISSI technology and to support Program Objective Memorandum (POM) and budget planning.

The DMS Target Architecture And Implementation Strategy (TAIS)

The TAIS was developed by the DMS Architecture Working Group and was sponsored by the ASDC3I. The TAIS defines terms, requirements, the baseline and objective architectures, and a high level transition strategy. The current version does not include a transition strategy for the tactical community of users.

Tactical DMS doctrine does not exist and probably will not for some time. Existing messaging doctrine, however, is found in FM 24-17. FM 24-17 is the doctrinal manual for the implementation and operation of the U.S. Army's formal and informal record traffic system. It includes formal messaging via the TYC-39 and AUTODIN system and informal messaging via the Tactical Facsimile and MSE Circuit Switch.

There have been several studies conducted with the purpose of determining the feasibility of extending the DMS into the tactical environment. Several studies looked primarily at the increased bandwidth imposed by the DMS protocols and their impact on the TPN.

Recently, the Executive Agent for Tactical Switched Systems was tasked by DISA to collate these studies and publish one set of results. GTE was also commissioned to study the feasibility of extending DMS to the battlefield. They completed an initial study in December 1994 titled Tactical Packet Network (TPN)/Defense Messaging System (DMS) Interoperability Study Report.[5] The Army Science Board (ASB) is currently studying the value of transitioning to an X.400 mail based system as opposed to remaining a Simple Mail Transfer Protocol (SMTP) based system.

Several DMS products have already been tested and more tests are planned. The Battle Command Battle Lab (BCBL) at Fort Gordon conducted testing of messaging components during the Secure Tactical Data Network (STDN) demonstration in 1993 and the Joint Warrior Interoperability Demonstration (JWID) in 1994 and 1995. The Digital Integration Lab (DIL) located at Fort Monmouth conducted tests in the spring of 1995 and plans to continue testing throughout the transition to DMS. The Joint Testing and Interoperability Center at Ft. Huachuca is the primary test center for compliance of all DMS products and will serve as the primary site for the Initial Operational Test and Evaluation (IOT&E) of DMS products in December 1995. Finally, Ft. Riley, Kansas was chosen by the Chief of Signal at Fort Gordon to participate in initial testing of the early DMS components. The agencies mentioned above have all published the results of past tests and will continue to publish the results of future tests.

Most of the working groups are formal, chartered organizations that are chaired by representatives from the Defense Information Systems Agency (DISA). One example is the Tactical

Working Group (TACWG). The TACWG is a joint working group that meets monthly. The purpose of this group is to develop joint architectures and transition strategies, identify requirements and identify and solve critical issues.

Others are informal and are under no legal charter. An example of one of the informal groups is the Tactical Army Working Group chaired by the Signal Center (SIGCEN) at Fort Gordon, Georgia. SIGCEN holds a quarterly working group designed to identify requirements and critical issues, develop the Army architecture and transition strategy, identify ongoing testing actions and results, and develop future testing plans. The first meeting of this group was in January, 1994 and the latest was October, 1995.

The last major information source for DMS is the World Wide Web (WWW). Many of the documents referenced above are posted there.

The majority of the literature focuses on the implementation of DMS and security products in the strategic and sustaining base environments. With the exception of the DMS Army Tactical Architecture and Transition Strategy, Annex F of the TAIS, a few studies, and test reports, very little has been written concerning the extension of DMS to the warfighter.

Endnotes

[1]Assistant Secretary of Defense for Command, Control, Communications and Intelligence, Memorandum for Secretaries of the Military Departments, Directors of the Defense Agencies, and the Joint Staff, Subject: Electronic Mail Policy, (Washington DC: 13 October 1992).

[2]Assistant Secretary of Defense for Command, Control, Communications and Intelligence, Memorandum for Secretaries of the Military Departments, Directors of the Defense Agencies, and the Joint Staff, Subject: Electronic Mail Policy, (Washington DC: 9 March 1995).

[3]Assistant Secretary of Defense for Command, Control, Communications and Intelligence, Memorandum for Secretaries of the Military Departments, Directors of the Defense Agencies, and the Joint Staff, Subject: Personal Computer Memory Card International Association (PCMCIA) Personal Computer and Workstation Contracts, (Washington DC: 7 July 1994).

[4]Headquarters, Electronic Systems Center (AFMC), Request For Proposal (RFP) No. F01620-93-R-A211 Defense Message System (DMS) - Government Open Systems Interconnection Profile (GOSIP) Acquisition, (Hanscomb AFB, MA: March 1994), p. C.1.

[5]GTE Government Systems Communication Systems Division, Tactical Packet Network (TPN)/Defense Message System (DMS) Interoperability Study Report (Draft), (19 December 1994).

APPENDIX B

METHODOLOGY

This thesis assesses the impact of extending DMS to the warfighter in the areas of doctrine, training, leader development, organizations, material and soldiers (DTLOMS). The DTLOMS are frequently used throughout TRADOC and acquisition communities to assess the impact of any new program, system, concept, equipment modification, personnel or organizational change.

Chapter 1 familiarizes the reader with the history of the DMS program, its purpose, concepts, and requirements. It identifies the assumptions this thesis makes; and identifies and defines the criteria used for assessing the impact of extending the Defense Message System to the battlefield. The method used to develop chapter one was a review of the available DMS documents, briefings, policies, and test reports.

Like many other programs, DMS is full of new equipment and terminology. Chapter 2 defines several key terms, however, this thesis assumes the reader has a basic knowledge and understanding of existing communications systems. Chapter 2 also describes the equipment that will be fielded for both the wide area network and the local area network.

Once the reader gains an understanding of the concepts, requirements, terms and components of DMS, he must become familiar with the Army's proposed architecture and transition strategy for implementing DMS on the battlefield. This transition strategy serves as the basis for deriving the impact of DMS across the full spectrum of the DTLOMS. This thesis analyzes the Army's strategy throughout each phase of the transition and highlights the key changes required to implement that portion of the DMS.

Chapter 4 analyzes the impact of extending DMS to the battlefield. As stated in chapter one, this thesis focuses primarily on the impact on the signal corps. The method used for assessing each area of the DTLOMS is as follows:

Doctrine

This thesis examined current messaging doctrine, DMS messaging doctrine already developed, and doctrine currently being written. The primary resources used were the U.S. Army Signal Center at Fort Gordon, Georgia, the Center for Army Doctrine at Fort Leavenworth, Kansas, the U.S. Army Information Systems Command at Fort Huachuca, Arizona, and the Defense Information Systems Agency in Washington, DC.

Training

To analyze the impact of DMS on training, this thesis determined the current training provided for messaging installers, planners, managers, and users. This includes an examination of current signal officer, signal noncommissioned officer, signal soldier and user training provided by institutional, sustainment and embedded training systems. The primary resource used was the Signal Center. This thesis also examined the training specified in the Defense Message System-Government Open System Interconnect Profile (GOSIP) Request For Proposal (RFP). This is the training the vendors are required to provide the DMS users, installers, maintainers and planners.

Leader Development

To analyze the impact on leader development, this thesis determined the roles and responsibilities leaders will play in the installation, operation, maintenance and management of future automation systems. The primary resource was FM 24-7 (Final Draft), ATCCS Systems Management Techniques. This thesis also examined the current system used by the Signal Corps to develop its leaders.

Organizations

To assess the impact on organizations, this thesis determined the number of soldiers required to operate the Tactical Record Traffic System used today. It then examines the manpower requirements for the DMS components and raises some issues related to organizational structure and manpower requirements.

Material

To assess the impact on material, this thesis examines the Army's tactical transition strategy. Further, it looks briefly at related programs and their relationship to the DMS program. A large portion of determining the impact on material is closely related to bandwidth. This thesis discusses the impact of the DMS protocols on the very limited resource of tactical bandwidth.

Soldiers

Finally, this thesis determines the impact on soldiers by examining the specific MOS requirements for DMS on the battlefield, and then looking at issues related to workload, additional training required and any retraining required.

Chapter 5 is the conclusion and recommendations for each area of the DTLOMS. The target audience for these recommendations is the system planners and combat developers at the U.S. Army Signal Center, Information Systems Command, and the Defense Information Systems Agency.

The Signal Center, USAISC, and DISA provided the majority of the documents used in the research. The internet also provided a means to gather data. Specifically, DISA instituted a DMS Homepage on the World Wide Web (WWW). Many documents to include the DMS Concept of Operation, Request For Proposal, the Target Architecture and Implementation Strategy (TAIS) and Service and Agency transition plans are located on the WWW. The Internet also provides access to the Web Home Pages at the Signal Center, the Defense Information Systems Agency, and the Information Systems Command.

BIBLIOGRAPHY

Periodicals

Cooper, Pat. "DOD Official Pushes Civilian Technology Lift." Defense News, Volume 11, no. 6 (1996): 16.

________. "U.S. Army Examines Initial Battlefield Imagery, Data." Defense News, Volume 10, Number 45 (1995): 22.

________. "U.S. Army Strives to Close Tactics, Technology Gap." Defense News, Volume 11, Number 5 (1996): 14.

________. "U.S. Military Eyes Security for Defense E-Mail System." Defense News, Volume 10, Number 43 (1995): 8.

Evans, Stanley E. "MOS 74B Information System Operator-Analyst." Army Communicator, Volume 20, Number 2 (1995): 41.

Gastyne, Fed de. "Interview: Emmitt Paige, Jr., Talks About DMS." Insight Magazine, (1995): 2.

Government Documents

Assistant Secretary of Defense, Command, Control, Communications and Intelligence. Memorandum for Secretaries of the Military Departments, Directors of the Defense Agencies, Directors of the DOD Field Activities, Director, Joint Staff, Subject: Electronic Messaging Policy Implementation Guidance. Washington, DC: Government Printing Office, 1995.

________. Memorandum for Secretaries of the Military Departments, Directors of the Defense Agencies, Directors of the DOD Field Activities, Director, Joint Staff, Subject: PCMCIA Card Slots in Personal Computer and Workstation Contracts. Washington, DC: Government Printing Office, 1994.

________. Memorandum for Director, National Security Agency. Use of FORTEZZA to protect classified information. Washington, DC: Government Printing Office, 1995.

Center for Information System Security Defense Information Systems Security Program. Department of Defense Goal Security Architecture Version 1.0. Ft. Meade, MD: Government Printing Office, 1993.

________. Department Of Defense Goal Security Architecture Transition Plan Version 1.0. Ft. Meade, MD: Government Printing Office, 1994.

Defense Communications Agency, Joint Tactical Command, Control, and Communications Agency. Functional C3 Interoperability Architecture for Land Combat Operations. Washington, DC: Government Printing Office, 1991.

Defense Information Systems Agency Center for Systems Engineering. Defense Information Infrastructure 1998 Target Security Architecture and Planning Guidance. MClean, VA: Government Printing Office, 1994.

Defense Information Systems Agency Joint Interoperability and Engineering Organization. Joint Task Force Tactical Communications Architecture. Washington, DC: Government Printing Office, 1995.

Defense Information Systems Agency. Allied Communication Publication 123 Tactical Requirements Analysis. MClean, VA: Government Printing Office, 1993.

________. Defense Message System Implementation Plan. FT. Huachuca, AZ: Government Printing Office, 1994.

________. Defense Message System (DMS) Required Operational Messaging Characteristics (ROMC). Arlington, VA: Government Printing Office, 1992.

________. Defense Message System Transition Plan Guidance. Arlington, VA: Government Printing Office, 1992.

________. DMS Capstone Material Fielding/Implementation Plan. Washington, DC: Government Printing Office, 1995.

________. DMS Joint Integrated Logistics Support Plan. Arlington, VA: Government Printing Office, 1995.

________. MISSI Implementation Guide. Washington, DC: Government Printing Office, 1994.

________. MISSI Implementation Plan. Washington, DC: Government Printing Office, 1994.

Deloria, Wayne C. Defense Message System Program Overview. Virginia: Defense Information Systems Agency, 1995.

Department of the Army, Headquarters U.S. Army Communication Electronics Command, Research, Development, and Engineering Center. Integrated Tactical to Strategic Data Network "Quick Fix" User Manual Version 1. Fort Monmouth, NJ: Executive Agent for Tactical Switched Systems, 1994.

Department of the Army. 93rd Signal Brigade After Action Report for Operations Desert Shield and Desert Storm. Germany: 93rd Signal Brigade, 1992.

________. C4I Technical Architecture. Washington, DC: Government Printing Office, 1995.

Director of Combat Developments. 16-17 May Tactical DMS Conference Notes. Fort Gordon, GA: Signal Center, 1995.

________. Army Common User System System Improvement Plan. FT. Gordon, GA: Signal Center, 1993.

Director of Information Systems Agency Joint Interoperability Engineering Organization. Multilevel Security in the Department Of Defense The Basics. Ft. Meade, MD: Government Printing Office, 1993.

Director of Information Systems for Command, Control, Communications, and Computers. Army Enterprise Strategy... The Vision, Washington, DC: Government Printing Office, 1993.

________. Army Enterprise Strategy, Washington, DC: Government Printing Office, 1994.

Directorate of Combat Developments. Modeling and Simulation ADO Study. Fort Gordon, GA: United States Army Signal Center, 1996.

________. Regimental Officer's Academy. Fort Gordon, GA: United States Army Signal Center, 1995.

________. Tactical Defense Message System Architecture and Transition Strategy. Fort Gordon, GA: United States Army Signal Center, 1996.

Executive Agent for Tactical Switched Systems. Defense Message System Proof Of Concept Tactical To Strategic Test Report. FT Monmouth, NJ: Government Printing Office, 1995.

GTE Government Systems. Tactical Packet Network/Defense Messaging System Interoperability and Tactical Packet Network/Command Post Architecture Interconnectivity Study Report. Needham, MA: GTE Communications Systems Division, 1995.

Headquarters, Department of the Army. Field Manual 100-5, Operations. Washington, DC: Government Printing Office, 1993.

________. Field Manual 24-17, Tactical Record Traffic System. Washington, DC: Government Printing Office, 1991.

________. Field Manual 24-7, Army Battle Command System (ABCS) Systems Management Techniques. Washington, DC: Government Printing Office, 1995.

Headquarters, Electronic Systems Center (AFMC). Request For Proposal (RFP) No. F01620-93-R-A211, Defense Message System (DMS) - Government Open Systems Interconnection Profile (GOSIP) Acquisition. Hanscomb AFB, MA: Government Printing Office, 1994.

________. Request For Proposal (RFP) No. F01620-93-R-A211, Defense Message System (DMS) - Government Open Systems Interconnection Profile (GOSIP) Acquisition Statement Of Work. Hanscomb AFB, MA: Government Printing Office, 1994.

Headquarters, U.S. Army Training and Doctrine Command. Operational Requirements Document (ORD) for Multilevel Security (MLS). Fort Monroe, VA: Government Printing Office, 1993.

Joint Chiefs of Staff. Multicommand Required Operational Capability (MROC) 3-88. Washington, DC: Government Printing Office, 1989.

Joint Staff. Change 1 to Defense Message System (DMS) Required Operational Messaging Characteristics (ROMC). Washington, DC: Government Printing Office, 1994.

________. Memorandum for Holders of MROC 3-88, Subject: Change 1 to MROC 3-88, "The Defense Message System." Washington, DC: Government Printing Office, 1993.

Loop, Tony. Warfighter Information Network and the Next Generation of Switches Using ATM Hub and ISDN White Paper. Fort Gordon, GA: Directorate of Combat Developments, 1995.

Mitre Corporation. DMS-Army Tactical Requirements Assessment. FT. Huachuca, AZ: Government Printing Office, 1994.

National Security Agency. Multilevel Information Systems Security Initiative Security Solutions for Today and Tomorrow. Ft. Meade, MD: Information Systems Security Office, 1995.

________. Multilevel Information Systems Security Initiative. Ft. Meade, MD: Information Systems Security Office, 1995.

________. Tech Trend Notes. Volume 2, Edition 3 (1993): 1-5.

________. Tech Trend Notes. Volume 3, Edition 3 (1994): 1-4.

Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Systems. The Defense Message System Target Architecture and Implementation Strategy. Washington, DC: Government Printing Office, 1993.

Training and Doctrine Command. Force Projection Army C4I Support. Ft. Monroe, VA: Government Printing Office, 1993.

U.S. Army Information Systems Command. Defense Message System Army (DMS Army) Tactical Architecture and Transition Strategy (Draft). Fort Huachuca, AZ: Government Printing Office, 1994.

U.S. Army Signal Center. Force XXI, The Signal Training Vision.

________. Signal Corps Pamphlet. Ft Gordon GA: Fort Gordon, 1994.

________. The Army Satellite Communications (SATCOM) Architecture. Fort Gordon, GA: TRADOC Systems Manager, 1996.

Volz, Richard. Tactical Internet for Task Force XXI White Paper. Fort Gordon GA: Directorate of Combat Developments, 1995.

Briefings

Bateman, Robert S. Asynchronous Transfer Mode (ATM) Technology and Applications Version 3.0. Atlanta, GA: AT&T Bell Laboratories, 1995.

Buchholz, Douglas D. Chief Signal Officer Notes. Fort Gordon, GA: United States Army Signal Center, 1995.

Garcia, Sherry. Army DMS Program Review. Ft Huachuca, AZ: United States Army Information Systems Command, 1995.

Hoh, Yan-Shek. Dr. Preliminary Analysis of DMS Overhead. MClean, VA: Mitre Corporation, 1994.

Loral Federal Systems. Defense Message System. Mclean, VA: Loral Federal Systems, 1995.

INITIAL DISTRIBUTION LIST

1. Combined Arms Research Library
   U.S. Army Command and General Staff College
   1 Reynolds Ave.
   Fort Leavenworth, KS 66027-1352

2. Defense Technical Information Center
   Cameron Station
   Alexandria, VA 22314

3. MAJ Howard R. Cuozzi
   CTAC
   USACGSC
   1 Reynolds Ave.
   Fort Leavenworth, KS 66027-1352

4. LTC Keith B. Harker
   LID
   USACGSC
   1 Reynolds Ave.
   Fort Leavenworth, KS 66027-1352

5. SFC John T. Broom
   CSI
   USACGSC
   1 Reynolds Ave.
   Fort Leavenworth, KS 66027-1352

6. U.S. Army Signal Center and Fort Gordon
   Directorate of Combat Developments
   Fort Gordon, GA 30905`

7. Mr. Edmund Kerut
   National Security Agency Liaison
   Signal Towers, 6th Floor
   Fort Gordon, GA 30905

8. Commander
   35th Signal Brigade
   Fort Bragg, NC 28307

9. Commander
   3rd Signal Brigade
   Fort Hood, TX 76544

10. Commander
    1st Signal Brigade
    APO AP 96205

11. Commander
    22nd Signal Brigade
    APO AE 09175

12. Commander
    7th Signal Brigade
    APO AE 09086

13. Commander
    11th Signal Brigade
    Fort, Huachuca, AZ 85613

14. Commander
    106th Signal Brigade
    APO AA 34004

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 25/APR/96

2. Thesis Author: MAJ Anthony E. Blando

3. Thesis Title: The Impact of Extending the Defense Message System to the Army Warfighter

4. Thesis Committee Members Signatures: ______________________

5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

A B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

S-----------SAMPLE---------SAMPLE---------SAMPLE----------SAMPLE-------S

Limitation Justification Statement	Chapter/Section	Page(s)
Direct Military Support (10)	Chapter 3	12
Critical Technology (3)	Sect. 4	31
Administrative Operational Use (7)	Chapter 2	13-32

----------SAMPLE---------SAMPLE----------SAMPLE----------SAMPLE-------

Fill in limitation justification for your thesis below:

Limitation Justification Statement	Chapter/Section	Page(s)

7. MMAS Thesis Author's Signature: ______________________

STATEMENT A: Approved for public release; distribution is unlimited. (Documents with this statement may be made available or sold to the general public and foreign nationals.)

STATEMENT B: Distribution authorized to U.S. Government agencies only (insert reason and date ON REVERSE OF THIS FORM). Currently used reasons for imposing this statement include the following:

1. Foreign Government Information. Protection of foreign information.

2. Proprietary Information. Protection of proprietary information not owned by the U.S. Government.

3. Critical Technology. Protection and control of critical technology including technical data with potential military application.

4. Test and Evaluation. Protection of test and evaluation of commercial production or military hardware.

5. Contractor Performance Evaluation. Protection of information involving contractor performance evaluation.

6. Premature Dissemination. Protection of information involving systems or hardware from premature dissemination.

7. Administrative/Operational Use. Protection of information restricted to official use or for administrative or operational purposes.

8. Software Documentation. Protection of software documentation--release only in accordance with the provisions of DoD Instruction 7930.2.

9. Specific Authority. Protection of information required by a specific authority.

10. Direct Military Support. To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize a U.S. military advantage.

STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT D: Distribution authorized to DoD and U.S. DoD contractors only: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT E: Distribution authorized to DoD only; (REASON AND DATE). Currently most used reasons are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

STATEMENT F: Further dissemination only as directed by (controlling DoD office and date), or higher DoD authority. Used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R.

STATEMENT X: Distribution authorized to U.S. Government agencies and private individuals of enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (insert).